Red Hat Enterprise Linux 5
5.8 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 5.8
Edition 8

Landmann

Red Hat Enterprise Linux 5 5.8 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 5.8
Edition 8

Landmann
rlandmann@redhat.com

Legal Notice

Copyright © 2011 Red Hat, Inc.

This document is licensed by Red Hat under the Creative Commons Attribution-ShareAlike 3.0 Unported License. If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, MetaMatrix, Fedora, the Infinity Logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

The Red Hat Enterprise Linux 5.8 Technical Notes list and document the changes made to the Red Hat Enterprise Linux 5 operating system and its accompanying applications between Red Hat Enterprise Linux 5.7 and minor release Red Hat Enterprise Linux 5.8.

Table of Contents

Preface **18**

Chapter 1. Technology Previews **19**

Chapter 2. Known Issues **24**
2.1. anaconda 24
2.2. autofs 28
2.3. cmirror 28
2.4. compiz 29
2.5. cpio 29
2.6. device-mapper-multipath 29
2.7. dmraid 30
2.8. dogtail 31
2.9. firstboot 31
2.10. gfs2-utils 31
2.11. gnome-volume-manager 32
2.12. initscripts 32
2.13. iscsi-initiator-utils 32
2.14. kernel-xen 33
2.15. kernel 34
2.16. kexec-tools 40
2.17. kvm 41
2.18. less 44
2.19. lftp 44
2.20. lvm2 45
2.21. mesa 45
2.22. mkinitrd 45
2.23. mod_revocator 46
2.24. openib 46
2.25. openmpi 46
2.26. perl-libxml-enno 47
2.27. pm-utils 47
2.28. rpm 47
2.29. redhat-release-notes 47
2.30. qspice 48
2.31. subscription-manager 48
2.32. systemtap 48
2.33. xen 49
2.34. virt-v2v 49
2.35. virtio-win 50
2.36. xorg-x11-drv-i810 50
2.37. xorg-x11-drv-nv 50
2.38. xorg-x11-drv-vesa 51
2.39. yaboot 51

Chapter 3. New Packages **52**
3.1. RHBA-2012:0286 — new package: binutils220 52
3.2. RHEA-2012:0224 — new package: iotop 52
3.3. RHEA-2012:0220 — new package: mysql-connector-odbc64 52
3.4. RHEA-2012:0171 — new package: pixman 52
3.5. RHEA-2012:0221 — new package: postgresql-odbc64 53
3.6. RHEA-2012:0183 — new package: python-ctypes 53

3.7. RHEA-2012:0172 — new package: spice-client 53
3.8. RHEA-2012:0170 — new package: spice-protocol 53
3.9. RHEA-2012:0290 — new package: subscription-manager-migration-data 54
3.10. RHEA-2012:0225 — new package: virt-who 54
3.11. RHEA-2012:0222 — new packages: unixODBC64 54

Chapter 4. Package Updates **55**
4.1. acl 55
4.1.1. RHBA-2012:0242 — acl bug fix update 55
Bug Fixes 55
4.2. acpid 55
4.2.1. RHBA-2011:1786 — acpid bug fix update 55
Bug Fixes 55
4.3. alsa-utils 56
4.3.1. RHEA-2012:0182 — alsa-utils enhancement update 56
Enhancement 56
4.4. anaconda 56
4.4.1. RHBA-2012:0197 — anaconda bug fix and enhancement update 56
Bug Fixes 56
Enhancement 58
4.5. aspell 59
4.5.1. RHBA-2011:1372 — aspell bug fix update 59
Bug Fix 59
4.6. aspell-sr 59
4.6.1. RHBA-2011:1368 — aspell-sr bug fix update 59
Bug Fix 59
4.7. audit 59
4.7.1. RHBA-2012:0265 — audit bug fix and enhancement update 59
Bug Fixes 60
Enhancement 60
4.8. autofs 60
4.8.1. RHBA-2011:1435 — autofs bug fix update 60
Bug Fix 61
4.8.2. RHBA-2011:1374 — autofs bug fix update 61
Bug Fix 61
4.8.3. RHBA-2011:1318 — autofs bug fix update 61
Bug Fix 61
4.8.4. RHBA-2012:0264 — autofs bug fix and enhancement update 61
Bug Fixes 62
Enhancement 63
4.9. bind 63
4.9.1. RHSA-2011:1458 — Important: bind security update 63
4.9.2. RHBA-2012:0254 — bind bug fix and enhancement update 64
Bug Fixes 64
Enhancement 65
4.10. bind97 65
4.10.1. RHSA-2011:1459 — Important: bind97 security update 65
4.11. binutils 65
4.11.1. RHBA-2012:0271 — binutils bug fix update 66
Bug Fixes 66
4.12. boost 66
4.12.1. RHBA-2011:1246 — boost bug fix update 66
Bug Fix 66
4.12.2. RHBA-2011:1149 — boost bug fix update 67
Bug Fix 67
4.12.3. RHSA-2012:0305 — Low: boost security and bug fix update 67

Bug Fixes 67
4.13. bootparamd 68
4.13.1. RHBA-2011:1190 — bootparamd bug fix update 68
Bug Fix 68
4.14. busybox 68
4.14.1. RHBA-2012:0026 — busybox bug fix update 68
Bug Fix 68
4.14.2. RHSA-2012:0308 — Low: busybox security and bug fix update 69
Bug Fixes 69
4.15. cdparanoia 69
4.15.1. RHBA-2012:0208 — cdparanoia bug fix update 69
Bug Fix 70
4.16. certmonger 70
4.16.1. RHBA-2011:1842 — certmonger bug fix update 70
Bug Fix 70
4.16.2. RHBA-2011:1238 — certmonger bug fix update 70
Bug Fix 70
4.16.3. RHBA-2012:0245 — certmonger bug fix and enhancement update 71
Bug Fixes 71
Enhancement 71
4.17. Cluster_Administration 71
4.17.1. RHBA-2012:0175 — Cluster_Administration bug fix and enhancement update 72
4.18. clustermon 72
4.18.1. RHBA-2012:0292 — clustermon bug-fix update 72
Bug Fixes 72
4.19. cman 72
4.19.1. RHBA-2012:0053 — cman bug fix update 72
Bug Fix 73
4.19.2. RHBA-2011:1337 — cman bug fix update 73
Bug Fix 73
4.19.3. RHEA-2011:1217 — cman enhancement update 73
Enhancement 73
4.19.4. RHBA-2012:0167 — cman bug fix and enhancement update 73
4.20. cmirror 76
4.20.1. RHBA-2012:0256 — cmirror bug fix update 76
Bug Fixes 76
4.21. comps-extras 76
4.21.1. RHBA-2012:0294 — comps-extras bug fix update 76
Bug Fix 76
4.22. conga 76
4.22.1. RHBA-2011:1421 — conga bug fix update 76
Bug Fix 77
4.22.2. RHSA-2012:0151 — Moderate: conga security, bug fix and enhancement update 77
4.23. crash 79
4.23.1. RHBA-2012:0203 — crash bug fix and enhancement update 79
Bug Fixes 79
4.24. cups 80
4.24.1. RHSA-2012:0302 — Low: cups security and bug fix update 80
Bug Fixes 80
4.25. curl 81
4.25.1. RHBA-2011:1188 — curl bug fix update 81
Bug Fix 81
4.25.2. RHBA-2012:0241 — curl bug fix and enhancement update 81
Bug Fixes 81
Enhancements 82

4.26. cvs 82
4.26.1. RHBA-2012:0253 — cvs bug fix update 82
Bug Fixes 83
4.27. cyrus-imapd 83
4.27.1. RHSA-2011:1508 — Moderate: cyrus-imapd security update 83
4.27.2. RHSA-2011:1317 — Important: cyrus-imapd security update 84
4.28. dapl 84
4.28.1. RHBA-2012:0252 — dapl bug fix update 84
Bug Fixes 84
4.29. dbus 85
4.29.1. RHSA-2011:1132 — Moderate: dbus security update 85
4.30. Deployment_Guide 86
4.30.1. RHBA-2012:0178 — Deployment_Guide bug fix and enhancement update 86
4.31. device-mapper 86
4.31.1. RHBA-2012:0219 — device-mapper bug fix and enhancement update 86
Bug Fix 86
4.32. device-mapper-multipath 86
4.32.1. RHBA-2011:1483 — device-mapper-multipath bug fix update 86
Bug Fix 87
4.32.2. RHBA-2011:1152 — device-mapper-multipath bug fix update 87
Bug Fix 87
4.32.3. RHBA-2012:0166 — device-mapper-multipath bug fix update 87
4.33. dhcp 89
4.33.1. RHSA-2011:1160 — Moderate: dhcp security update 89
4.33.2. RHBA-2012:0194 — dhcp bug fix update 90
Bug Fix 90
4.34. dovecot 90
4.34.1. RHSA-2011:1187 — Moderate: dovecot security update 90
4.35. ecryptfs-utils 91
4.35.1. RHSA-2011:1241 — Moderate: ecryptfs-utils security update 91
4.35.2. RHBA-2011:1503 — ecryptfs-utils bug fix update 92
Bug Fixes 92
4.36. esound 93
4.36.1. RHBA-2012:0295 — esound bug fix update 93
Bug Fix 93
4.37. fcoe-utils 93
4.37.1. RHBA-2012:0230 — fcoe-utils package update 93
Bug Fixes 93
4.38. fetchmail 93
4.38.1. RHBA-2011:1540 — fetchmail bug fix update 93
Bug Fix 94
4.39. file 94
4.39.1. RHBA-2012:0201 — file bug fix update 94
Bug Fixes 94
4.40. firefox 96
4.40.1. RHSA-2012:0079 — Critical: firefox security update 96
4.40.2. RHSA-2011:1437 — Critical: firefox security update 97
4.40.3. RHSA-2011:1341 — Critical: firefox security update 97
4.40.4. RHSA-2011:1268 — Important: firefox security update 98
4.40.5. RHSA-2011:1242 — Important: firefox security update 99
4.40.6. RHSA-2011:1164 — Critical: firefox security update 99
4.41. firstboot 100
4.41.1. RHBA-2012:0278 — firstboot bug fix update 100
Bug Fixes 100
4.42. foomatic 101

4.42.1. RHSA-2011:1109 — Moderate: foomatic security update 101
4.43. freeipmi 101
4.43.1. RHBA-2011:1499 — freeipmi bug fix update 101
Bug Fixes 101
4.44. freeradius2 102
4.44.1. RHBA-2012:0196 — freeradius2 bug fix and enhancement update 102
Bug Fixes 102
4.45. freetype 103
4.45.1. RHSA-2011:1455 — Important: freetype security update 103
4.45.2. RHSA-2011:1402 — Important: freetype security update 103
4.46. gamin 104
4.46.1. RHBA-2011:1537 — gamin bug fix update 104
Bug Fix 104
4.47. gawk 104
4.47.1. RHBA-2011:1486 — gawk bug fix update 104
Bug Fix 104
4.48. gcc 105
4.48.1. RHBA-2012:0258 — gcc bug fix update 105
Bug Fixes 105
4.49. gcc44 106
4.49.1. RHEA-2012:0272 — gcc44 enhancement update 106
Enhancement 106
4.50. gdb 106
4.50.1. RHBA-2011:1129 — gdb bug fix update 106
Bug Fix 106
4.50.2. RHBA-2012:0238 — gdb bug fix update 107
Bug Fixes 107
4.51. gdm 107
4.51.1. RHBA-2012:0282 — gdm bug fix update 107
Bug Fixes 108
4.52. gfs-kmod 108
4.52.1. RHBA-2012:0277 — gfs-kmod bug fix update 108
Bug Fixes 108
4.53. gfs-utils 109
4.53.1. RHBA-2012:0276 — gfs-utils bug fix update 109
Bug Fixes 109
4.54. gfs2-utils 109
4.54.1. RHBA-2012:0269 — gfs2-utils bug fix and enhancement update 109
Bug Fixes 109
Enhancement 110
4.55. ghostscript 110
4.55.1. RHSA-2012:0095 — Moderate: ghostscript security update 110
4.55.2. RHBA-2011:1286 — ghostscript bug fix update 111
Bug Fixes 112
4.55.3. RHBA-2012:0284 — ghostscript bug fix and enhancement update 112
Bug Fixes 112
4.56. glibc 113
4.56.1. RHSA-2012:0126 — Moderate: glibc security update 113
4.56.2. RHBA-2011:1488 — glibc bug fix update 114
Bug Fix 114
4.56.3. RHBA-2012:0260 — glibc bug fix update 114
Bug Fixes 114
4.57. Global_File_System 116
4.57.1. RHBA-2012:0176 — Global_File_System bug fix and enhancement update 116
4.58. gnome-screensaver 116

4.58.1. RHBA-2012:0008 — gnome-screensaver bug fix update 116
Bug Fix 116
4.58.2. RHBA-2012:0002 — gnome-screensaver bug fix update 116
Bug Fix 117
4.59. gnome-system-monitor 117
4.59.1. RHBA-2012:0212 — gnome-system-monitor bug fix and enhancement update 117
Bug Fix 117
Enhancement 117
4.60. gpart 117
4.60.1. RHBA-2011:1376 — gpart bug fix update 117
Bug Fix 118
4.61. groff 118
4.61.1. RHBA-2011:1484 — groff bug fix update 118
Bug Fix 118
4.62. gtk2 118
4.62.1. RHBA-2011:1795 — gtk2 bug fix update 118
Bug Fix 118
4.63. hmaccalc 119
4.63.1. RHBA-2011:1462 — hmaccalc bug fix update 119
4.64. httpd 119
4.64.1. RHSA-2011:1392 — Moderate: httpd security and bug fix update 119
Bug Fix 119
4.64.2. RHSA-2011:1245 — Important: httpd security update 120
4.64.3. RHBA-2012:0261 — httpd bug fix and enhancement update 120
Bug Fixes 120
4.65. hwdata 121
4.65.1. RHEA-2012:0235 — hwdata enhancement update 121
Enhancements 121
4.66. ibutils 122
4.66.1. RHSA-2012:0311 — Low: ibutils security and bug fix update 122
Bug Fix 122
4.67. icu 122
4.67.1. RHSA-2011:1815 — Moderate: icu security update 122
4.68. ifd-egate 123
4.68.1. RHBA-2012:0214 — ifd-egate bug fix update 123
Bug Fixes 123
4.69. ImageMagick 123
4.69.1. RHSA-2012:0301 — Low: ImageMagick security and bug fix update 123
Bug Fixes 124
4.70. initscripts 124
4.70.1. RHSA-2012:0312 — Low: initscripts security and bug fix update 125
Bug Fixes 125
4.71. ipa-client 126
4.71.1. RHBA-2011:1841 — ipa-client bug fix update 126
Bug Fix 126
4.71.2. RHBA-2011:1290 — ipa-client bug fix update 126
Bug Fix 126
4.71.3. RHBA-2012:0190 — ipa-client bug fix update 126
Bug Fixes 127
4.72. iproute 128
4.72.1. RHBA-2011:1453 — iproute bug fix update 128
Bug Fixes 128
4.73. iprutils 128
4.73.1. RHEA-2012:0185 — iprutils enhancement update 128
Enhancement 128

4.74. iptables 129
4.74.1. RHBA-2012:0255 — iptables bug fix and enhancement update 129
Bug Fixes 129
4.75. iscsi-initiator-utils 130
4.75.1. RHBA-2012:0263 — iscsi-initiator-utils bug fix and enhancement update 130
Bug Fixes 130
Enhancements 130
4.76. java-1.6.0-openjdk 130
4.76.1. RHSA-2011:1380 — Critical: java-1.6.0-openjdk security update 131
4.76.2. RHBA-2012:0314 — java-1.6.0-openjdk bug fix and enhancement update 132
Bug Fix 133
Enhancements 133
4.77. kdelibs 133
4.77.1. RHSA-2011:1385 — Moderate: kdelibs and kdelibs3 security update 133
4.78. kernel 133
4.78.1. RHSA-2012:1445 — Moderate: kernel security and bug fix update 134
4.78.2. RHSA-2012:1174 — Low: kernel security and bug fix update 136
4.78.3. RHSA-2012:0690 — Important: kernel security and bug fix update 138
4.78.4. RHSA-2012:0480 — Important: kernel security, bug fix, and enhancement update 140
4.78.5. RHSA-2012:0150 — Moderate: Red Hat Enterprise Linux 5.8 kernel security, bug fix, and enhancement update 142
4.78.6. RHSA-2012:0107 — Important: kernel security and bug fix update 154
4.78.7. RHSA-2012:0007 — Important: kernel security, bug fix, and enhancement update 156
4.78.8. RHSA-2011:1479 — Important: kernel security, bug fix, and enhancement update 157
4.78.9. RHSA-2011:1386 — Important: kernel security, bug fix, and enhancement update 158
4.78.10. RHSA-2011:1212 — Important: kernel security and bug fix update 160
Bug Fixes 160
4.79. kexec-tools 161
4.79.1. RHEA-2012:0090 — kexec-tools enhancement update 162
Enhancement 162
4.79.2. RHSA-2012:0152 — Moderate: kexec-tools security, bug fix and enhancement update 162
4.80. krb5 165
4.80.1. RHSA-2011:1851 — Critical: krb5 security update 165
4.80.2. RHSA-2012:0306 — Low: krb5 security and bug fix update 165
Bug Fixes 166
4.81. ksh 166
4.81.1. RHBA-2012:0159 — ksh bug fix and enhancement update 167
4.82. kudzu 170
4.82.1. RHEA-2012:0232 — kudzu bug fix and enhancement update 171
Bug Fix 171
Enhancement 171
4.83. kvm 171
4.83.1. RHSA-2012:0051 — Important: kvm security update 171
4.83.2. RHSA-2012:0149 — Moderate: kvm security, bug fix and enhancement update 172
4.84. less 174
4.84.1. RHBA-2011:1468 — less bug fix update 174
4.85. lftp 174
4.85.1. RHBA-2011:1541 — lftp bug fix update 174
Bug Fixes 174
4.86. libcxgb3 175
4.86.1. RHBA-2012:0184 — libcxgb3 bug fix and enhancement update 175
4.87. libdhcp 175
4.87.1. RHBA-2012:0193 — libdhcp bug fix update 175
Bug Fix 175
4.88. libexif 176

4.88.1. RHBA-2011:1472 — libexif bug fix update 176
Bug Fix 176
4.89. libhbaapi 176
4.89.1. RHBA-2011:1425 — libhbaapi package updated 176
Bug Fixes 176
4.90. libmlx4 177
4.90.1. RHBA-2012:0270 — libmlx4 bug fix update 177
Bug Fix 177
4.91. libpng 177
4.91.1. RHSA-2011:1104 — Moderate: libpng security update 177
4.92. libusb 178
4.92.1. RHBA-2011:1498 — libusb bug fix 178
Bug Fix 178
4.93. libvirt 178
4.93.1. RHBA-2012:0248 — libvirt bug fix update 178
Bug Fixes 178
4.94. libvorbis 179
4.94.1. RHSA-2012:0136 — Important: libvorbis security update 179
4.95. libX11 180
4.95.1. RHBA-2011:1351 — libX11 bug fix update 180
Bug Fix 180
4.96. libXcursor 180
4.96.1. RHBA-2011:1538 — libXcursor bug fix update 180
Bug Fix 180
4.97. libXfont 180
4.97.1. RHSA-2011:1154 — Important: libXfont security update 180
4.98. libxml2 181
4.98.1. RHSA-2012:0017 — Important: libxml2 security update 181
4.98.2. RHBA-2011:1416 — libxml2 bug fix update 182
Bug Fix 182
4.99. lsof 182
4.99.1. RHBA-2012:0206 — lsof bug fix and enhancement update 182
Bug Fixes 183
Enhancements 183
4.100. ltrace 183
4.100.1. RHBA-2011:1473 — ltrace bug fix update 183
Bug Fix 183
4.101. lvm2 184
4.101.1. RHBA-2012:0056 — lvm2 bug fix update 184
Bug Fix 184
4.101.2. RHBA-2011:1222 — lvm2 bug fix update 184
Bug Fix 184
4.101.3. RHBA-2012:0161 — lvm2 bug fix and enhancement update 184
4.102. lvm2-cluster 187
4.102.1. RHBA-2012:0223 — lvm2-cluster bug fix and enhancement update 187
Enhancements 188
4.103. man-pages 188
4.103.1. RHBA-2011:1461 — man-pages bug fix and enhancement update 188
Bug Fixes 188
Enhancements 189
4.104. man-pages-ja 189
4.104.1. RHBA-2011:1367 — man-pages-ja bug fix update 189
Bug Fix 189
4.105. man-pages-overrides 189
4.105.1. RHBA-2012:0259 — man-pages-overrides bug fix update 189

Bug Fixes 189
4.106. mesa 190
4.106.1. RHBA-2012:0288 — mesa bug fix update 190
Bug Fixes 190
4.107. microcode_ctl 191
4.107.1. RHBA-2012:0189 — microcode_ctl bug fix and enhancement update 191
Bug Fixes 191
Enhancement 191
4.108. mkinitrd 191
4.108.1. RHBA-2011:1491 — mkinitrd bug fix update 192
Bug Fix 192
4.108.2. RHBA-2012:0157 — mkinitrd bug fix update 192
4.109. mod_auth_kerb 194
4.109.1. RHBA-2012:0057 — mod_auth_kerb bug fix update 194
Bug Fix 194
4.110. mod_revocator 194
4.110.1. RHBA-2012:0247 — mod_revocator bug fix update 194
Bug Fixes 195
4.111. mrtg 195
4.111.1. RHBA-2011:1493 — mrtg bug fix update 195
Bug Fixes 195
4.112. mysql 196
4.112.1. RHSA-2012:0127 — Moderate: mysql security update 196
4.113. mysql-connector-odbc 196
4.113.1. RHEA-2012:0227 — mysql-connector-odbc bug fix update 196
4.114. MySQL-python 197
4.114.1. RHBA-2012:0181 — MySQL-python bug fix update 197
4.115. net-snmp 197
4.115.1. RHBA-2011:1216 — net-snmp bug fix update 197
Bug Fix 197
4.115.2. RHBA-2012:0165 — net-snmp bug fix update 197
4.116. net-tools 200
4.116.1. RHBA-2012:0188 — net-tools bug fix update 200
Bug Fixes 200
4.117. netpbm 201
4.117.1. RHSA-2011:1811 — Important: netpbm security update 201
4.117.2. RHBA-2012:0287 — netpbm bug fix update 201
Bug Fixes 202
4.118. nfs-utils 202
4.118.1. RHSA-2012:0310 — Low: nfs-utils security, bug fix, and enhancement update 202
Bug Fixes 203
Enhancement 204
4.119. nfs-utils-lib 204
4.119.1. RHEA-2012:0299 — nfs-utils-lib enhancement update 204
Enhancement 204
4.120. nfs4-acl-tools 204
4.120.1. RHBA-2012:0296 — nfs4-acl-tools bug fix update 204
Bug Fix 204
4.121. nss 205
4.121.1. RHSA-2011:1444 — Important: nss security update 205
4.121.2. RHSA-2011:1282 — Important: nss and nspr security update 206
4.121.3. RHBA-2012:0291 — nss and nspr bug fix update 206
Bug Fixes 206
4.122. nss_ldap 207
4.122.1. RHBA-2011:1413 — nss_ldap bug fix update 207

Bug Fix 207
4.122.2. RHBA-2012:0268 — nss_ldap bug fix and enhancement update 207
Bug Fixes 208
4.123. ntp 208
4.123.1. RHBA-2011:1454 — ntp bug fix update 208
Bug Fix 208
4.124. oddjob 209
4.124.1. RHBA-2011:1492 — oddjob bug fix update 209
Bug Fix 209
4.125. openais 209
4.125.1. RHBA-2011:1487 — openais bug fix update 209
Bug Fixes 209
4.125.2. RHBA-2011:1428 — openais bug fix update 210
Bug Fixes 210
4.125.3. RHBA-2011:1262 — openais bug fix update 210
Bug Fix 210
4.125.4. RHBA-2012:0180 — openais bug fix and enhancement update 211
Bug Fixes 211
Enhancement 212
4.126. openCryptoki 212
4.126.1. RHBA-2012:0239 — openCryptoki bug fix update 212
Bug Fixes 212
4.127. OpenIPMI 213
4.127.1. RHBA-2011:1107 — OpenIPMI bug fix update 213
Bug Fix 213
4.128. openldap 213
4.128.1. RHBA-2011:1482 — openldap bug fix update 213
Bug Fix 214
4.128.2. RHEA-2011:1345 — openldap bug fix and enhancement update 214
Bug Fixes 214
4.128.3. RHBA-2012:0155 — openldap bug fix and enhancement update 215
4.129. openmotif 217
4.129.1. RHBA-2011:1451 — openmotif bug fix update 217
Bug Fixes 217
4.130. openscap 218
4.130.1. RHEA-2012:0209 — openscap bug fix and enhancement update 218
4.131. openssh 218
4.131.1. RHBA-2011:1195 — openssh bug fix update 218
Bug Fix 218
4.131.2. RHBA-2012:0237 — openssh bug fix and enhancement update 219
Bug Fixes 219
Enhancement 220
4.132. openssl 220
4.132.1. RHSA-2012:0060 — Moderate: openssl security update 220
4.132.2. RHBA-2012:0229 — openssl bug fix and enhancement update 221
Bug Fix 221
Enhancements 221
4.133. openswan 222
4.133.1. RHSA-2011:1422 — Moderate: openswan security update 222
4.133.2. RHBA-2012:0211 — openswan bug fix and enhancement update 222
Bug Fixes 223
4.134. oprofile 224
4.134.1. RHEA-2012:0267 — oprofile enhancement update 224
Enhancements 224
4.135. pam_krb5 224

4.135.1. RHBA-2012:0246 — pam_krb5 bug fix update 224
Bug Fix 224
4.136. pam_pkcs11 225
4.136.1. RHBA-2012:0215 — pam_pkcs11 bug fix update 225
Bug Fix 225
4.137. pango 225
4.137.1. RHSA-2011:1326 — Moderate: pango security update 225
4.138. parted 226
4.138.1. RHBA-2012:0192 — parted bug fix update 226
Bug Fixes 226
4.139. pciutils 226
4.139.1. RHBA-2012:0251 — pciutils bug fix and enhancement update 226
Bug Fix 226
Enhancements 227
4.140. pdksh 227
4.140.1. RHBA-2011:1394 — pdksh bug fix update 227
4.141. perl 227
4.141.1. RHSA-2011:1797 — Moderate: perl security update 227
4.141.2. RHBA-2012:0199 — perl bug fix update 228
Bug Fixes 228
4.142. perl-XML-SAX 229
4.142.1. RHBA-2011:1446 — perl-XML-SAX bug fix update 229
Bug Fixes 230
4.143. php 230
4.143.1. RHSA-2012:0093 — Critical: php security update 230
4.143.2. RHBA-2012:0249 — php bug fix and enhancement update 230
Bug Fixes 231
Enhancement 231
4.144. php53 232
4.144.1. RHSA-2012:0092 — Critical: php53 security update 232
4.144.2. RHSA-2011:1423 — Moderate: php53 and php security update 232
4.144.3. RHBA-2012:0266 — php53 bug fix update 233
Bug Fixes 234
4.145. piranha 234
4.145.1. RHBA-2012:0262 — piranha bug fix update 234
Bug Fixes 234
Enhancement 234
4.146. poppler 235
4.146.1. RHBA-2012:0236 — poppler bug fix update 235
Bug Fixes 235
4.147. postgresql 236
4.147.1. RHSA-2011:1377 — Moderate: postgresql security update 236
4.147.2. RHBA-2011:1447 — postgresql bug fix update 236
Bug Fix 236
4.148. postgresql84 237
4.148.1. RHSA-2011:1378 — Moderate: postgresql84 security update 237
4.149. ppc64-utils 237
4.149.1. RHEA-2012:0186 — ppc64-utils bug fix and enhancement update 238
Bug Fixes 238
Enhancements 238
4.150. procinfo 238
4.150.1. RHBA-2012:0021 — procinfo bug fix update 238
Bug Fix 239
4.151. procps 239
4.151.1. RHEA-2011:1497 — procps enhancement update 239

Enhancement 239
4.152. python 239
4.152.1. RHBA-2011:1319 — python bug fix update 239
Bug Fix 239
4.152.2. RHBA-2012:0297 — python bug fix update 240
Bug Fixes 240
4.153. python-rhsm 240
4.153.1. RHBA-2012:0280 — python-rhsm bug fix update 240
Bug Fixes 240
4.154. python-virtinst 241
4.154.1. RHBA-2012:0233 — python-virtinst bug fix update 241
Bug Fixes 241
4.155. PyXML 242
4.155.1. RHBA-2011:1460 — PyXML bug fix update 242
Bug Fixes 242
4.156. qt4 242
4.156.1. RHSA-2011:1324 — Moderate: qt4 security update 242
4.157. rdesktop 243
4.157.1. RHBA-2012:0213 — rdesktop bug fix update 243
Bug Fixes 243
4.158. redhat-release 243
4.158.1. RHEA-2012:0315 — redhat-release enhancement update 243
4.159. redhat-release-notes 244
4.159.1. RHEA-2012:0298 — redhat-release-notes enhancement update 244
4.160. rgmanager 244
4.160.1. RHBA-2012:0066 — rgmanager bug fix update 244
Bug Fix 244
4.160.2. RHBA-2012:0163 — rgmanager bug fix and enhancement update 244
4.161. rhn-client-tools 247
4.161.1. RHBA-2012:0250 — rhn-client-tools bug fix update 247
Bug Fixes 247
4.162. rhnlib 248
4.162.1. RHBA-2012:0240 — rhnlib bug fix update 248
Bug Fix 248
4.163. rhpl 248
4.163.1. RHBA-2012:0275 — rhpl bug fix update 248
Bug Fix 248
4.164. rng-utils 249
4.164.1. RHEA-2012:0293 — rng-utils enhancement update 249
Enhancement 249
4.165. rpm 249
4.165.1. RHSA-2011:1349 — Important: rpm security update 249
4.165.2. RHBA-2012:0283 — rpm bug fix and enhancement update 250
Bug Fixes 250
Enhancements 251
4.166. rsh 251
4.166.1. RHBA-2011:1429 — rsh bug fix update 251
Bug Fix 251
4.167. rsync 251
4.167.1. RHBA-2011:1112 — rsync bug fix update 251
Bug Fix 251
4.168. rsyslog 252
4.168.1. RHBA-2012:0228 — rsyslog bug fix and enhancement update 252
Bug Fixes 252
Enhancement 253

4.169. ruby 253
4.169.1. RHBA-2012:0218 — ruby bug fix update 253
Bug Fixes 254
4.170. s390utils 254
4.170.1. RHBA-2012:0243 — s390utils bug fix update 254
Bug Fixes 254
4.171. sabayon 256
4.171.1. RHBA-2012:0202 — sabayon bug fix update 256
Bug Fixes 256
4.172. samba 256
4.172.1. RHSA-2011:1219 — Moderate: samba security update 256
4.172.2. RHSA-2012:0313 — Low: samba security, bug fix, and enhancement update 257
Bug Fix 258
4.173. samba3x 258
4.173.1. RHSA-2011:1220 — Moderate: samba3x security update 258
4.173.2. RHBA-2012:0156 — samba3x bug fix and enhancement update 259
4.174. sblim 262
4.174.1. RHBA-2012:0191 — sblim bug fix and enhancement update 262
Bug Fixes 262
Enhancements 263
4.175. scsi-target-utils 263
4.175.1. RHBA-2012:0279 — scsi-target-utils bug fix update 263
Bug Fix 264
4.176. selinux-policy 264
4.176.1. RHBA-2012:0106 — selinux-policy bug fix update 264
Bug Fix 264
4.176.2. RHBA-2012:0158 — selinux-policy bug fix and enhancement update 264
4.177. sendmail 268
4.177.1. RHBA-2011:1127 — sendmail bug fix update 268
Bug Fix 268
4.178. setroubleshoot 268
4.178.1. RHBA-2012:0146 — setroubleshoot bug fix update 268
Bug Fix 268
4.179. setup 268
4.179.1. RHBA-2012:0198 — setup bug fix and enhancement update 269
Bug Fixes 269
4.180. shadow-utils 270
4.180.1. RHBA-2012:0244 — shadow-utils bug fix update 270
Bug Fixes 270
4.181. smartmontools 271
4.181.1. RHBA-2011:1784 — smartmontools bug fix update 271
Bug Fix 271
4.182. sos 271
4.182.1. RHBA-2011:1535 — sos bug fix update 271
Bug Fix 271
4.182.2. RHSA-2012:0153 — Low: sos security, bug fix and enhancement update 272
4.183. spice-client 275
4.183.1. RHBA-2012:0147 — spice-client bug fix update 275
Bug Fix 275
4.184. spice-usb-share 276
4.184.1. RHEA-2012:0174 — spice-usb-share enhancement update 276
Enhancement 276
4.185. spice-xpi 276
4.185.1. RHBA-2012:0316 — spice-xpi bug fix and enhancement update 276
Enhancement 276

4.186. squirrelmail 276
4.186.1. RHSA-2012:0103 — Moderate: squirrelmail security update 276
4.187. sssd 278
4.187.1. RHBA-2012:0164 — sssd bug fix and enhancement update 278
4.188. subscription-manager 286
4.188.1. RHBA-2012:0148 — subscription-manager bug fix update 286
Bug Fix 286
4.188.2. RHBA-2012:0154 — subscription-manager bug fix and enhancement update 286
4.189. sudo 288
4.189.1. RHSA-2012:0309 — Low: sudo security and bug fix update 288
Bug Fixes 289
4.190. syslinux 290
4.190.1. RHBA-2012:0207 — syslinux bug fix update 290
Bug Fix 290
4.191. system-config-bind 290
4.191.1. RHBA-2011:1505 — system-config-bind bug fix update 290
4.192. system-config-cluster 290
4.192.1. RHBA-2012:0210 — system-config-cluster bug fix and enhancement update 291
Bug Fix 291
Enhancement 291
4.193. system-config-date 291
4.193.1. RHBA-2011:1490 — system-config-date bug fix update 291
Bug Fix 291
4.194. system-config-display, 291
4.194.1. RHBA-2012:0285 — system-config-display, rhpxl, and pyxf86config bug fix update 292
Bug Fixes 292
4.195. system-config-network 292
4.195.1. RHBA-2012:0231 — system-config-network bug fix and enhancement update 292
4.196. system-config-printer 293
4.196.1. RHSA-2011:1196 — Moderate: system-config-printer security update 294
4.197. system-switch-mail 294
4.197.1. RHBA-2011:1489 — system-switch-mail bug fix update 294
Bug Fix 294
4.198. systemtap 294
4.198.1. RHSA-2011:1089 — Moderate: systemtap security update 294
4.198.2. RHBA-2012:0200 — systemtap bug fix update 295
Bug Fixes 295
4.199. tog-pegasus 296
4.199.1. RHBA-2012:0257 — tog-pegasus bug fix update 296
Bug Fixes 296
Enhancement 297
4.200. tomcat5 297
4.200.1. RHSA-2011:1845 — Moderate: tomcat5 security update 297
4.201. udev 298
4.201.1. RHBA-2011:1448 — udev bug fix update 298
Bug Fix 298
4.202. unixODBC 298
4.202.1. RHEA-2012:0226 — unixODBC enhancement update 298
Enhancement 298
4.203. util-linux 299
4.203.1. RHSA-2012:0307 — Low: util-linux security, bug fix, and enhancement update 299
Bug Fixes 299
Enhancements 300
4.204. virt-manager 300
4.204.1. RHBA-2012:0216 — virt-manager bug fix update 300

Bug Fixes 300
4.205. virtio-win 301
4.205.1. RHBA-2011:1288 — virtio-win floppy disk update 301
4.206. Virtualization_Guide 301
4.206.1. RHBA-2012:0177 — Virtualization_Guide bug fix and enhancement update 301
4.207. vixie-cron 301
4.207.1. RHSA-2012:0304 — Low: vixie-cron security, bug fix, and enhancement update 301
Bug Fixes 302
Enhancement 303
4.208. vsftpd 303
4.208.1. RHBA-2012:0187 — vsftpd bug fix and enhancement update 303
Bug Fixes 303
Enhancements 304
4.209. xen 304
4.209.1. RHSA-2011:1401 — Moderate: xen security and bug fix update 304
Bug Fixes 304
4.209.2. RHBA-2012:0160 — xen bug fix and enhancement update 305
4.210. xenpv-win 308
4.210.1. RHBA-2012:0195 — xenpv-win bug fix update 308
Bug Fixes 308
4.211. xinetd 309
4.211.1. RHBA-2012:0217 — xinetd bug fix and enhancement update 309
Bug Fix 309
Enhancement 309
4.212. xkeyboard-config 310
4.212.1. RHEA-2011:1153 — xkeyboard-config enhancement update 310
Enhancement 310
4.212.2. RHEA-2012:0173 — xkeyboard-config enhancement update 310
Enhancement 310
4.213. xmlrpc-c 310
4.213.1. RHEA-2011:1237 — xmlrpc-c enhancement update 310
Enhancement 310
4.213.2. RHBA-2012:0179 — xmlrpc-c bug fix update 311
Bug Fixes 311
4.214. xorg-x11-drv-i810 311
4.214.1. RHBA-2012:0289 — xorg-x11-drv-i810 bug fix update 311
Bug Fix 311
4.215. xorg-x11-drv-mga 311
4.215.1. RHBA-2012:0234 — xorg-x11-drv-mga bug fix and enhancement update 311
Bug Fixes 312
Enhancement 312
4.216. xorg-x11-drv-sis 312
4.216.1. RHBA-2011:1420 — xorg-x11-drv-sis bug fix update 312
Bug Fix 312
4.217. xorg-x11-server 312
4.217.1. RHSA-2011:1359 — Moderate: xorg-x11-server security update 313
4.217.2. RHSA-2012:0303 — Low: xorg-x11-server security and bug fix update 313
Bug Fixes 313
4.218. xulrunner 315
4.218.1. RHSA-2012:0143 — Critical: xulrunner security update 315
4.219. yaboot 315
4.219.1. RHBA-2012:0300 — yaboot bug fix update 315
Bug Fix 315
4.220. yp-tools 316
4.220.1. RHEA-2012:0204 — yp-tools enhancement update 316

Enhancement 316
4.221. ypserv 316
4.221.1. RHBA-2012:0205 — ypserv bug fix and enhancement update 316
Bug Fixes 316
Enhancements 317
4.222. yum 318
4.222.1. RHBA-2012:0273 — yum bug fix and enhancement update 318
Bug Fix 318
4.223. yum-rhn-plugin 318
4.223.1. RHBA-2011:1281 — yum-rhn-plugin bug fix update 318
Bug Fixes 318
4.223.2. RHBA-2011:1198 — yum-rhn-plugin bug fix update 319
Bug Fix 319
4.223.3. RHBA-2012:0162 — yum-rhn-plugin bug fix update 319
4.224. yum-utils 321
4.224.1. RHBA-2012:0281 — yum-utils bug fix and enhancement update 321
Bug Fixes 321
Enhancement 322
4.225. zsh 322
4.225.1. RHBA-2012:0274 — zsh bug fix update 322
Bug Fixes 323

Package Manifest **324**
A.1. Server 324
A.1.1. Added Packages 324
A.1.2. Dropped Packages 325
A.1.3. Updated Packages 325
A.2. Client 415
A.2.1. Added Packages 415
A.2.2. Dropped Packages 417
A.2.3. Updated Packages 417

Revision History **502**

Preface

The *Red Hat Enterprise Linux 5.8 Technical Notes* list and document the changes made to the Red Hat Enterprise Linux 5 operating system and its accompanying applications between minor release Red Hat Enterprise Linux 5.7 and minor release Red Hat Enterprise Linux 5.8.

For system administrators and others planning Red Hat Enterprise Linux 5.8 upgrades and deployments, the *Red Hat Enterprise Linux 5.8 Technical Notes* provide a single, organized record of the bugs fixed in, features added to, and Technology Previews included with this new release of Red Hat Enterprise Linux.

For auditors and compliance officers, the *Red Hat Enterprise Linux 5.8 Technical Notes* provide a single, organized source for change tracking and compliance testing.

For every user, the *Red Hat Enterprise Linux 5.8 Technical Notes* provide details of what has changed in this new release.

The *Red Hat Enterprise Linux 5.8 Technical Notes* also include, as an Appendix, the Red Hat Enterprise Linux 5.8 Package Manifest: a listing of every changed package in this release.

Chapter 1. Technology Previews

Technology Preview features are currently *not* supported under Red Hat Enterprise Linux subscription services, may not be functionally complete, and are generally not suitable for production use. However, these features are included as a customer convenience and to provide the feature with wider exposure.

Customers may find these features useful in a non-production environment. Customers are also free to provide feedback and functionality suggestions for a Technology Preview feature before it becomes fully supported. Erratas will be provided for high-severity security issues.

During the development of a Technology Preview feature, additional components may become available to the public for testing. It is the intention of Red Hat to fully support Technology Preview features in a future release.

DFS

Starting with Red Hat Enterprise Linux 5.3, CIFS supports Distributed File System (DFS) as a Technology Preview.

Package: *kernel-2.6.18-308*

CDTB

CTDB is a clustered database based on Samba's Trivial Database (TDB). The *ctdb* package is a cluster implementation used to store temporary data. If an application is already using TBD for temporary data storage, it can be very easily converted to be cluster-aware and use CTDB.

Package: *ctdb-1.0.112-1*

Kerberos support for CIFS mounts

In Red Hat Enterprise Linux 5.8, users can use their Kerberos credentials to perform a CIFS mount.

Package: *samba-client-3.0.33-3.37*

Brocade BFA/BNA Fibre-Channel/FCoE driver

The **bfa**/**bna** driver for Brocade Fibre Channel Host Bus adapters is considered a Technology Preview in Red Hat Enterprise Linux 5.8. (BZ#475695)

Package: *kernel-2.6.18-308*

FreeIPMI

FreeIPMI is included in as a Technology Preview. FreeIPMI is a collection of Intelligent Platform Management IPMI system software. It provides in-band and out-of-band software, along with a development library conforming to the Intelligent Platform Management Interface (IPMI v1.5 and v2.0) standards.

For more information about FreeIPMI, refer to http://www.gnu.org/software/freeipmi/

Package: *freeipmi-0.5.1-7*

TrouSerS and tpm-tools

TrouSerS and **tpm-tools** are included in this release to enable use of *Trusted Platform*

Module (TPM) hardware. TPM hardware features include (among others):

- Creation, storage, and use of RSA keys securely (without being exposed in memory)
- Verification of a platform's software state using cryptographic hashes

TrouSerS is an implementation of the Trusted Computing Group's Software Stack (TSS) specification. You can use TrouSerS to write applications that make use of TPM hardware. **`tpm-tools`** is a suite of tools used to manage and utilize TPM hardware.

For more information about TrouSerS, refer to http://trousers.sourceforge.net/.

Packages: *tpm-tools-1.3.1-1*, *trousers-0.3.1-4*

eCryptfs

eCryptfs is a stacked cryptographic file system for Linux. It mounts on individual directories in existing mounted lower file systems such as EXT3; there is no need to change existing partitions or file systems in order to start using **eCryptfs**. **eCryptfs** is released as a Technology Preview for Red Hat Enterprise Linux 5.8.

For more information about **eCryptfs**, refer to http://ecryptfs.sf.net. You can also refer to http://ecryptfs.sourceforge.net/README and http://ecryptfs.sourceforge.net/ecryptfs-faq.html for basic setup information.

Package: *ecryptfs-utils-75-8*

Stateless Linux

Stateless Linux, included as a Technology Preview, is a new way of thinking about how a system should be run and managed, designed to simplify provisioning and management of large numbers of systems by making them easily replaceable. This is accomplished primarily by establishing prepared system images which get replicated and managed across a large number of stateless systems, running the operating system in a read-only manner (refer to **`/etc/sysconfig/readonly-root`** for more details).

In its current state of development, the Stateless features are subsets of the intended goals. As such, the capability remains as Technology Preview.

Red Hat recommends that those interested in testing stateless code join the stateless-list@redhat.com mailing list.

The enabling infrastructure pieces for Stateless Linux were originally introduced in Red Hat Enterprise Linux 5.

AIGLX

AIGLX is a Technology Preview feature of the otherwise fully supported X server. It aims to enable GL-accelerated effects on a standard desktop. The project consists of the following:

- A lightly modified X server.
- An updated Mesa package that adds new protocol support.

By installing these components, you can have GL-accelerated effects on your desktop with very few changes, as well as the ability to enable and disable them at will without replacing your X server. AIGLX also enables remote GLX applications to take advantage of hardware GLX acceleration.

Packages: X Window System group of packages.

FireWire

The **firewire-sbp2** module is included in this update as a Technology Preview. This module enables connectivity with FireWire storage devices and scanners.

At present, FireWire does not support the following:

- IPv4
- *pcilynx* host controllers
- multi-LUN storage devices
- non-exclusive access to storage devices

In addition, the following issues still exist in FireWire:

- a memory leak in the **SBP2** driver may cause the machine to become unresponsive.
- a code in this version does not work properly in big-endian machines. This could lead to unexpected behavior in PowerPC.

Package: *kernel-2.6.18-308*

Device Failure Monitoring of RAID sets

Device Failure Monitoring, using the **dmraid** and **dmevent_tool** tools, is included in Red Hat Enterprise Linux 5.8 as a Technology Preview. This Technology Preview provides the ability to watch and report device failures on component devices of RAID sets.

Packages: *dmraid-1.0.0.rc13-65*, *dmraid-events-1.0.0.rc13-65*

SGPIO Support for dmraid

Serial General Purpose Input Output (SGPIO) is an industry standard communication method used between a main board and a variety of internal and external hard disk drive bay enclosures. This method can be used to control LED lights on an enclosure through the AHCI driver interface.

In this release, SGPIO support in **dmraid** is included as a technology preview. This will allow **dmraid** to work properly with disk enclosures.

Package: *dmraid-1.0.0.rc13-65*

Kernel Tracepoint Facility

In this update, the kernel marker/tracepoint facility remains a Technology Preview. This interface adds static probe points into the kernel, for use with tools such as **SystemTap**.

Package: *kernel-2.6.18-308*

Software based Fibre Channel over Ethernet (FCoE)

The Fibre Channel over Ethernet (FCoE) driver (fcoe.ko), along with libfc, provides the ability to run FCoE over a standard Ethernet card. This capability is provided as a Technology Preview in Red Hat Enterprise Linux 5.8.

To enable this feature, you must login by writing the network interface name to the **/sys/module/fcoe/parameters/create** file, for example:

```
~]# echo eth6 > /sys/module/fcoe/parameters/create
```

To logout, write the network interface name to the **/sys/module/fcoe/parameters/destroy** file, for example:

```
~]# echo eth6 > /sys/module/fcoe/parameters/destroy
```

For further information on software based FCoE refer to: http://www.open-fcoe.org/open-fcoe/wiki/quickstart.

Red Hat Enterprise Linux 5.8 provides full support for FCoE on three specialized hardware implementations. These are: Cisco **fnic** driver, the Emulex **lpfc** driver, and the Qlogic **qla2xx** driver.

Package: *kernel-2.6.18-308*

iSER Support

iSER support, allowing for block storage transfer across a network and provided by the *scsi-target-utils* package, remains a Technology Preview in Red Hat Enterprise Linux 5.8. In this release, single portal and multiple portals on different subnets are supported. There are known issues related to using multiple portals on the same subnet.

To set up the iSER target component install the *scsi-target-utils* and *libibverbs-devel* packages. The library package for the InfiniBand hardware that is being used is also required. For example: host channel adapters that use the **cxgb3** driver the **libcxgb3** package is needed, and for host channel adapters using the **mthca** driver the **libmthca** package is needed.

There is also a known issue relating to connection timeouts in some situations. Refer to BZ#470627 for more information on this issue.

Package: *scsi-target-utils-1.0.14-2*, other above-mentioned system-specific packages

cman fence_virsh fence agent

The fence_virsh fence agent is provided in this release of Red Hat Enterprise Linux as a Technology Preview. fence_virsh provides the ability for one guest (running as a domU) to fence another using the libvirt protocol. However, as fence_virsh is not integrated with cluster-suite it is not supported as a fence agent in that environment.

Package: *cman-2.0.115-96*

glibc new MALLOC behavior

The upstream **glibc** has been changed to enable higher scalability across many sockets and cores. This is done by assigning threads their own memory pools and by avoiding locking in some situations. The amount of additional memory used for the memory pools (if any) can be controlled using the environment variables **MALLOC_ARENA_TEST** and **MALLOC_ARENA_MAX**.

MALLOC_ARENA_TEST specifies that a test for the number of cores is performed once the number of memory pools reaches this value. **MALLOC_ARENA_MAX** sets the maximum number of memory pools used, regardless of the number of cores.

The **glibc** in the Red Hat Enterprise Linux 5.8 release has this functionality integrated as a Technology Preview of the upstream malloc. To enable the per-thread memory pools the environment variable **MALLOC_PER_THREAD** needs to be set in the environment. This environment variable will become obsolete when this new malloc behavior becomes default in future releases. Users experiencing contention for the malloc resources could try enabling this option.

Package: *glibc-2.5-81*

Chapter 2. Known Issues

2.1. anaconda

The *anaconda* packages provide the installation program used by Red Hat Enterprise Linux to identify and configure the hardware, and to create the appropriate file systems for the system's architecture, as well as to to install the operating system software.

- After a reboot of a freshly-installed system, the IP over Infiniband (IPoIB) interface fails to come up automatically as Anaconda fails to manually enable the **openibd** init script. To work around this issue, enable the **openibd** init script in the post section of the Kickstart file prior to the installation of the system:

  ```
  %post
  chkconfig --level 12345 openibd on
  ```

- When installing Red Hat Enterprise Linux 5.8 on a machine that had previously used a GPT partitioning table, Anaconda does not provide the option to remove the previous disk layout and is unable to remove the previously used GPT partitioning table. To work around this issue, switch to the tty2 terminal (using **CTRL**+**ALT**+**F2**), execute the following command, and restart the installation process:

  ```
  dd if=/dev/zero of=/dev/USED_DISK count=512
  ```

- Starting with Red Hat Enterprise Linux 5.2, to boot with **ibft**, the iSCSI boot firmware table support, use the **ip=ibft** option as the network install option:

  ```
  ip=<ip>
      IP to use for a network installation, use 'dhcp' for DHCP.
  ```

  By default, the installer waits 5 seconds for a network device with a link. If an iBFT network device is not detected in this time, you may need to specify the ***linksleep=SECONDS*** parameter in addition to the ***ip=ibft*** parameter by replacing ***SECONDS*** with an integer specifying the number of seconds the installer should wait, for example:

  ```
  linksleep=10
  ```

- Setting the ***dhcptimeout=0*** parameter does not mean that DHCP will disable timeouts. If the user requires the clients to wait indefinitely, the ***dhcptimeout*** parameter needs to be set to a large number.
- When starting an installation on IBM S/390 systems using SSH, re-sizing the terminal window running the SSH client may cause the installer to unexpectedly exit. Once the installer has started in the SSH session, do not resize the terminal window. If you want to use a different size terminal window during installation, re-size the window before connecting to the target system via SSH to begin installation.
- Installing on June with a RAID backplane on Red Hat Enterprise Linux 5.7 and later does not work properly. Consider the following example: a test system which had two disks with two redundant paths to each disk was set up:

  ```
  mpath0: sdb, sdd
  mpath1: sda, sdc
  ```

In the above setup, Anaconda created the PReP partition on mpath0 (sdb/sdd), but set the bootlist to boot from sda. To work around this issue, follow these steps:

1. Add **mpath** to the append line in the **/etc/yaboot.conf** file.
2. Use the **--ondisk=mapper/mpath0** in all **part** directives of the kickstart file.
3. Add the following script to the **%post** section of the kickstart file.

```
%post
# Determine the boot device
device=;

# Set the bootlist in NVRAM
if [ "z$device" != "z" ]; then
bootlist -m normal $device;

# Print the resulting boot list in the log
bootlist -m normal -o;
bootlist -m normal -r;
else
echo "Could not determine boot device!";
exit 1;
fi
```

The above script simply ensures that the bootlist is set to boot from the disk with the PReP partition.

- Mounting an NFS volume in the rescue environment requires **portmap** to be running. To start **portmap**, run:

```
/usr/sbin/portmap
```

Failure to start **portmap** will return the following NFS mount errors:

```
sh-3.2# mount 192.168.11.5:/share /mnt/nfs
mount: Mounting 192.168.11.5:/share on /mnt/nfs failed: Input/output error
```

- The order of device names assigned to USB attached storage devices is not guaranteed. Certain USB attached storage devices may take longer to initialize than others, which can result in the device receiving a different name than you expect (for example, **sdc** instead of **sda**).

  During installation, be sure to verify the storage device size, name, and type when configuring partitions and file systems.
- **anaconda** occasionally crashes while attempting to install on a disk containing partitions or file systems used by other operating systems. To workaround this issue, clear the existing partition table using the command:

```
clearpart --initlabel [disks]
```

(BZ#530465)

- Performing a System z installation, when the **install.img** is located on direct access storage device (DASD) disk, causes the installer to crash, returning a backtrace. **anaconda** is attempting to re-write (commit) all disk labels when partitioning is complete, but is failing because the partition is busy. To work around this issue, a non-DASD source should be used for **install.img**. (BZ#455929)
- When installing to an **ext3** or **ext4** file system, **anaconda** disables periodic file system checking. Unlike **ext2**, these file systems are journaled, removing the need for a periodic file system check. In

the rare cases where there is an error detected at runtime or an error while recovering the file system journal, the file system check will be run at boot time. (BZ#513480)

- Red Hat Enterprise Linux 5 does not support having a separate **/var** on a network file system (**nfs**, **iSCSI** disk, **nbd**, etc.) This is because **/var** contains the utilities required to bring up the network, for example **/var/lib/dhcp**. However, you may have **/var/spool**, **/var/www** or the like on a separate network disk, just not the complete /var file system. (BZ#485478)
- When using rescue mode on an installation which uses iSCSI drives which were manually configured during installation, the automatic mounting of the root file system does not work. You must configure iSCSI and mount the file systems manually. This only applies to manually configured iSCSI drives; iSCSI drives which are automatically detected through iBFT are fully supported in rescue mode.

  To rescue a system which has **/** on a non-iBFT configured iSCSI drive, choose to skip the mounting of the root file system when asked, and then follow the steps below:

```
$TARGET_IP: IP address of the iSCSI target (drive)
$TARGET_IQN: name of the iSCSI target as printed by the discovery command
$ROOT_DEV: devicenode (/dev/.....) where your root fs lives
```

  1. Define an initiator name:

```
$ mkdir /etc/iscsi
$ cat << EOF>> /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.1994-05.com.fedora:d62f2d7c09f
EOF
```

  2. Start iscsid:

```
$ iscsid
```

  3. Discover and login to target:

```
$ iscsiadm -m discovery -t st -p $TARGET_IP
$ iscsiadm -m node -T $TARGET_IQN -p $TARGET_IP --login
```

  4. If the iSCSI LUN is part of a LVM Logical volume group:

```
$ lvm vgscan
$ lvm vgchange -ay
```

  5. Mount your **/** partition:

```
$ mount /dev/path/to/root /mnt/sysimage
$ mount -t bind /dev /mnt/sysimage/dev
$ mount -t proc proc /mnt/sysimage/proc
$ mount -t sysfs sysfs /mnt/sysimage/sys
```

  6. Now you can **chroot** to the root file system of your installation if wanted

```
$ chroot /mnt/sysimage /bin/su -
```

- When installing KVM or Xen guests, always create a partition for the guest disk, or create an LVM volume. Guests should not be installed to block devices or raw disk devices. Anaconda includes disk label duplication avoidance code, but when installing within a VM, it has no visibility to the disk labels elsewhere on the host and cannot detect duplicates.

If guest file systems, especially the root file system, are directly visible to the host, a host OS reboot may inadvertently parse the partition table and mount the guest file systems. This can lead to highly undesirable outcomes.

- The minimum memory requirement when installing all Red Hat Enterprise Linux packages (i.e. ***** or **@everything** is listed in the **%packages** section of the **kickstart** file) on a fully virtualized Itanium guest is 768MB. After installation, the memory allocated to the guest can be lowered to the desired amount.
- Upgrading a system using Anaconda is not possible if the system is installed on disks attached using zFCP or iSCSI (unless booted from the disk using a network adapter with iBFT). Such disks are activated after Anaconda scans for upgradable installations and are not found. To update please use the Red Hat Network with the hosted Web user interface, a Red Hat Network Satellite, the local graphical Updater, or the yum command line.
- Anaconda's graphical installer fails to start at the default 800x600 resolution on systems utilizing Intel Graphics Device Next Generation (IGDNG) devices. To work around this issue, ensure anaconda uses a higher resolution by passing the parameters **resolution=1024x768** or **resolution=1280x1024** to the installer using the boot command line.
- The NFS default for RHEL5 is **locking**. Therefore, to mount **nfs** shares from the **%post** section of anaconda, use the **mount -o nolock,udp** command to start the locking daemon before using **nfs** to mount shares. (BZ#426053)
- If you are using the Virtualized kernel when upgrading from Red Hat Enterprise Linux 5.0 to a later 5.x release, you must reboot after completing the upgrade. You should then boot the system using the updated Virtualized kernel.

  The hypervisor ABI changes in an incompatible way between Red Hat Enterprise Linux 5 and 5.1. If you do not boot the system after upgrading from Red Hat Enterprise Linux 5.0 using the updated Virtualized kernel, the upgraded Virtualization RPMs will not match the running kernel. (BZ#251669)
- When upgrading from Red Hat Enterprise Linux 4.6 to Red Hat Enterprise Linux 5.1 or later, **gcc4** may cause the upgrade to fail. As such, you should manually remove the *gcc4* package before upgrading. (BZ#432773)
- When provisioning guests during installation, the **RHN tools for guests** option will not be available. When this occurs, the system will require an additional entitlement, separate from the entitlement used by **dom0**.

  To prevent the consumption of additional entitlements for guests, install the **rhn-virtualization-common** package manually before attempting to register the system to Red Hat Network. (BZ#431648)
- When installing Red Hat Enterprise Linux 5 on a guest, the guest is configured to explicitly use a temporary installation kernel provided by **dom0**. Once installation finishes, it can then use its own bootloader. However, this can only be achieved by forcing the guest's first reboot to be a shutdown.

  As such, when the **Reboot** button appears at the end of the guest installation, clicking it shuts down the guest, but does not reboot it. This is an expected behavior.

  Note that when you boot the guest after this it will then use its own bootloader.
- Using the **swap --grow** parameter in a **kickstart** file without setting the **--maxsize** parameter at the same time makes anaconda impose a restriction on the maximum size of the swap partition. It does not allow it to grow to fill the device.

  For systems with less than 2GB of physical memory, the imposed limit is twice the amount of physical memory. For systems with more than 2GB, the imposed limit is the size of physical memory plus 2GB. (BZ#462734)
- Existing encrypted block devices that contain **vfat** file systems will appear as type **foreign** in the partitioning interface; as such, these devices will not be mounted automatically during system boot. To ensure that such devices are mounted automatically, add an appropriate entry for them to

/etc/fstab. For details on how to do so, refer to **man fstab**. (BZ#467202)

- When using anaconda's automatic partitioning on an IBM System p partition with multiple hard disks containing different Linux distributions, the anaconda installer may overwrite the bootloaders of the other Linux installations although their hard disks have been unchecked. To work around this, choose manual partitioning during the installation process.

The following known issue applies to the PowerPC architecture:

- The minimum RAM required to install Red Hat Enterprise Linux 5.8 is 1GB; the recommended RAM is 2GB. If a machine has less than 1GB RAM, the installation process may hang.

  Furthermore, PowerPC-based machines that have only 1GB of RAM experience significant performance issues under certain RAM-intensive workloads. For a Red Hat Enterprise Linux 5.8 system to perform RAM-intensive processes optimally, 4GB of RAM is recommended. This ensures the system has the same number of physical pages as was available on PowerPC machines with 512MB of RAM running Red Hat Enterprise Linux 4.5 or earlier.

The following known issue applies to the IBM System z architecture:

- Installation on a machine with existing Linux or non-Linux file systems on DASD block devices may cause the installer to halt. If this happens, it is necessary to clear out all existing partitions on the DASD devices you want to use and restart the installer.

The following known issue applies to the Itanium architecture:

- If your system only has 512MB of RAM, attempting to install Red Hat Enterprise Linux 5.4 may fail. To prevent this, perform a base installation first and install all other packages after the installation finishes. (BZ#435271)

2.2. autofs

The autofs utility controls the operation of the automount daemon. The automount daemon automatically mounts file systems when you use them, and unmounts them when they are not busy.

- Starting with Red Hat Enterprise Linux 5.4, behavior of the **umount -l** autofs command has changed. For more information, refer to BZ#452122.

  Previously, the **umount -l** would unmount all autofs-managed mounts and autofs internal mounts at start-up, and then mounted all autofs mounts again as a part of the start-up procedure. As a result, the execution of the external **umount -l** command was not needed.

  The previous autofs behavior can be used via the following commands:

  ```
  ~]# service autofs forcerestart
  ```

  or

  ```
  ~]# service autofs forcestart
  ```

2.3. cmirror

The *cmirror* packages provide user-level utilities for managing cluster mirroring.

- Due to limitations in the cluster infrastructure, cluster mirrors greater than 1.5TB cannot be created with the default region size. If larger mirrors are required, the region size should be increased from its default (512kB), for example:

```
# -R <region_size_in_MiB>
lvcreate -m1 -L 2T -R 2 -n mirror vol_group
```

Failure to increase the region size will result in the LVM creation process hanging and may cause other LVM commands to hang. (BZ#514814)

2.4. compiz

Compiz is an OpenGL-based window and compositing manager.

- Running **rpmbuild** on the **compiz** source RPM will fail if any KDE or **qt** development packages (for example, **qt-devel**) are installed. This is caused by a bug in the **compiz** configuration script.

  To work around this, remove any KDE or **qt** development packages before attempting to build the **compiz** package from its source RPM. (BZ#444609)

2.5. cpio

The GNU **cpio** utility copies files into or out of a *cpio* or *tar* archive.

- The **cpio** utility uses a default block size of 512 bytes for I/O operations. This may not be supported by certain types of tape devices. If a tape device does not support this block size, **cpio** fails with the following error message:

  ```
  cpio: read error: Cannot allocate memory
  ```

  To work around this issue, modify the default block size with the **--block-size long** option, or use the **-B** option to set the block size to 5120 bytes. When the block size supported by the tape device is provided, the **cpio** utility works as expected. (BZ#573943)

2.6. device-mapper-multipath

The *device-mapper-multipath* packages provide tools to manage multipath devices using the device-mapper multipath kernel module.

- By default, the **multipathd** service starts up before the **iscsi** service. This provides multipathing support early in the bootup process and is necessary for multipathed iSCSI SAN boot setups. However, once started, the **multipathd** service adds paths as informed about them by udev. As soon as the **multipathd** service detects a path that belongs to a multipath device, it creates the device. If the first path that multipathd notices is a passive path, it attempts to make that path active. If it later adds a more optimal path, **multipathd** activates the more optimal path. In some cases, this can cause a significant overhead during a startup.

  If you are experiencing such performance problems, define the **multipathd** service to start after the **iscsi** service. This does not apply to systems where the root device is a multipathed iSCSI device, since it the system would become unbootable. To move the service start time run the following commands:

  ```
  ~]# mv /etc/rc5.d/S06multipathd /etc/rc5.d/S14multipathd
  ~]# mv /etc/rc3.d/S06multipathd /etc/rc3.d/S14multipathd
  ```

  To restore the original start time, run the following command:

```
~]# chkconfig multipathd resetpriorities
```

(BZ#500998)

- Running the **multipath** command with the **-ll** option can cause the command to hang if one of the paths is on a blocking device. Note that the driver does not fail a request after some time if the device does not respond.

  This is caused by the cleanup code, which waits until the path checker request either completes or fails. To display the current **multipath** state without hanging the command, use **multipath -l** instead. (BZ#214838)

2.7. dmraid

The *dmraid* packages contain the ATARAID/DDF1 activation tool that supports RAID device discovery, RAID set activation, and displays properties for ATARAID/DDF1 formatted RAID sets on Linux kernels using device-mapper.

- The installation procedure stores the name of RAID volume and partition in an initscript. When the system boots, dmraid enables the RAID partition (that are named implicitly in the init script. This action functions until the volume and partition names are changed. In these cases, the system may not boot, and the user is given an option to reboot system and start the rebuild procedure in OROM.

  OROM changes the name of RAID volume (as seen by dmraid) and dmraid cannot recognize the array identified by previous name stored in initscript. The system no longer boots from RAID partition, since it is not enabled by dmraid. In case of RAID 1 (mirror), the system may be booted from disk that is part of RAID volume. However, dmraid does not allow to active or rebuild the volume which component in mounted.

  To work around this issue, do not rebuild the RAID array in OROM. Start the rebuild procedure by dmraid in the operating system, which performs all the steps of rebuilding. dmraid does not change the RAID volume name, therefore the system can be booted from RAID array without the need of init script modification.

  To modify init script after OROM has started rebuild:

  1. Start the system in rescue mode from the installation disk, skip finding and mounting previous installations.
  2. At the command line, find and enable the raid volume that is to be booted from (the RAID volume and partitions will be activated)

     ```
     ~]# dmraid -ay isw_effjffhbi_Volume0
     ```

  3. Mount the root partition:

     ```
     ~]# mkdir /tmp/raid
     ~]# mount /dev/mapper/isw_effjffhbi_Volume0p1 /tmp/raid
     ```

  4. Decompress the boot image:

     ```
     ~]# mkdir /tmp/raid/tmp/image
     ~]# cd /tmp/raid/tmp/image
     ~]# gzip -cd /tmp/raid/boot/inird-2.6.18-155.el5.img | cpio -imd –
     quiet
     ```

  5. Change the names of the RAID volumes in the initscript to use the new names of RAID:

```
~]# dmraid –ay –I –p –rm_partition “/dev/mapper/isw_effjffhbi_Volume0”
~]# kpartx –a –p p “/dev/mapper/isw_effjffhbi_Volume0”
~]# mkrtootdev –t ext3 –o defaults,ro
/dev/mapper/isw_effjffhbi_Volume0p1
```

6. Compress and copy initrd image with the modified init script to the boot directory

```
~]# cd /tmp/raid/tmp/image
~]# find . –print | cpio –c –o | gzip -9 > /tmp/raid/boot/inird-
2.6.18-155.el5.img
```

7. Unmount the raid volume and reboot the system:

```
~]# umount /dev/mapper/isw_effjffhbi_Volume0p1
~]# dmraid -an
```

2.8. dogtail

dogtail is a GUI test tool and automation framework that uses assistive technologies to communicate with desktop applications.

- Attempting to run **sniff** may result in an error. This is because some required packages are not installed with **dogtail**. (BZ#435702)

  To prevent this from occurring, install the following packages manually:
  - *librsvg2*
  - *ghostscript-fonts*
  - *pygtk2-libglade*

2.9. firstboot

The **firstboot** utility runs after installation. It guides the user through a series of steps that allows for easier configuration of the machine.

The following known issue applies to the IBM System z architecture:

- The *IBM System z* does not provide a traditional Unix-style physical console. As such, Red Hat Enterprise Linux 5.8 for the *IBM System z* does not support the *firstboot* functionality during initial program load.

  To properly initialize setup for Red Hat Enterprise Linux 5.8 on the *IBM System z*, run the following commands after installation:
  - **/usr/bin/setup** — provided by the **setuptool** package.
  - **/usr/bin/rhn_register** — provided by the **rhn-setup** package.

  (BZ#217921)

2.10. gfs2-utils

The *gfs2-utils* packages provide the user-level tools necessary to mount, create, maintain and test **GFS2** file systems.

If gfs2 is used as the root file system, the first boot attempt will fail with the error message "**fsck.gfs2: invalid option -- a**". To work around this issue:

1. Enter the root password when prompted.
2. Mount the root file system manually:

```
~]# mount -o remount,rw /dev/VolGroup00/LogVol00 /
```

3. Edit the /etc/fstab file from:

```
/dev/VolGroup00/LogVol00 / gfs2 defaults 1 1
```

to

```
/dev/VolGroup00/LogVol00 / gfs2 defaults 1 0
```

4. Reboot the system.

Important

Note, however that using **GFS2** as the root file system is unsupported.

2.11. gnome-volume-manager

The GNOME Volume Manager monitors volume-related events and responds with user-specified policy. The GNOME Volume Manager can automount hot-plugged drives, automount inserted removable media, autorun programs, automatically play audio CDs and video DVDs, and automatically import photos from a digital camera.

- Removable storage devices (such as CDs and DVDs) do not automatically mount when you are logged in as root. As such, you will need to manually mount the device through the graphical file manager.

  Alternatively, you can run the following command to mount a device to **/media**:

```
mount /dev/[device name] /media
```

2.12. initscripts

The *initscripts* package contains system scripts to boot your system, change runlevels, activate and deactivate most network interfaces, and shut the system down cleanly.

- On systems with more than two encrypted block devices, anaconda has a option to provide a global passphrase. The init scripts, however, do not support this feature. When booting the system, entering each individual passphrase for all encrypted devices will be required. (BZ#464895)
- Boot-time logging to **/var/log/boot.log** is not available in Red Hat Enterprise Linux 5.7. (BZ#223446, BZ#210136)

2.13. iscsi-initiator-utils

The *iscsi* package provides the server daemon for the iSCSI protocol, as well as the utility programs used to manage it. iSCSI is a protocol for distributed disk access using SCSI commands sent over Internet Protocol networks.

- iSCSI iface binding is not supported during install or boot. The initiator only supports the ability to log into target portals using the default behavior where the initiator uses the network routing table to decide which NIC to use.

  To work around this limitation, booting or installation can be done using the default behavior. After the iscsi and iscsid services start, the iscsi service can log into the target using iSCSI iface binding. This however, will leave an extra session using the default behavior, and it has to be manually logged out using the following command:

  ```
  iscsiadm -m node -T target -p ip -I default -u
  ```

  (BZ#500273)

2.14. kernel-xen

- Xen guests will not boot using configurations that bind multiple virtualized CPUs to a single CPU. (BZ#570056)
- The Xen hypervisor will not start when booting from an iSCSI disk. To work around this issue, disable the Xen hypervisor's EDD feature with the "edd=off" kernel parameter. For example:

  ```
  kernel /xen.gz edd=off
  ```

  (BZ#568336)
- With certain hardware, **blktap** may not function as expected, resulting in slow disk I/O causing the guest to operate slowly also. To work around this issue, guests should be installed using a physical disk (i.e. a real partition or a logical volume). (BZ#545692)
- When booting paravirtualized guests that support gigabyte page tables (i.e. a Fedora 11 guest) on Red Hat Enterprise Linux 5.7 Xen, the domain may fail to start if more than 2047MB of memory is configured for the domain. To work around this issue, pass the "**nogbpages**" parameter on the guest kernel command-line. (BZ#502826)
- Boot parameters are required to enable SR/IOV Virtual Function devices. SR/IOV Virtual Function devices can only be accessed if the parameter pci_pt_e820_access=on is added to the boot stanza in the /boot/grub/grub.conf file. For example:

  ```
  title Red Hat Enterprise Linux Server (2.6.18-152.el5xen)
  root (hd0,1)
  kernel /xen.gz-2.6.18-152.el5 com1=115200,8n1 console=com1 iommu=1
  module /vmlinuz-2.6.18-152.el5xen ro root=LABEL=/ console=ttyS0,115200
  pci_pt_e820_access=on
  ```

  This enables the MMCONF access method for the PCI configuration space, a requirement for VF device support
- Diskette drive media will not be accessible when using the virtualized kernel. To work around this, use a USB-attached diskette drive instead.

  Note that diskette drive media works well with other non-virtualized kernels. (BZ#401081)
- Fully virtualized guests cannot correct for time lost due to the domain being paused and unpaused. Being able to correctly track the time across pause and unpause events is one of the advantages of paravirtualized kernels. This issue is being addressed upstream with replaceable timers, so fully virtualized guests will have paravirtualized timers. Currently, this code is under development upstream and should be available in later versions of Red Hat Enterprise Linux. (BZ#422531)

The following known issue applies to the Intel 64 and AMD64 architectures:

- Upgrading a host (**dom0**) system to Red Hat Enterprise Linux 5.7 may render existing Red Hat Enterprise Linux 5.4 SMP paravirtualized guests unbootable. This is more likely to occur when the host system has more than 4GB of RAM.

  To work around this, boot each Red Hat Enterprise Linux 5.4 guest in single CPU mode and upgrade its kernel to the latest version (for Red Hat Enterprise Linux 5.4.z). (BZ#253087, BZ#251013)

The following known issues apply to the Itanium architecture:

- On some *Itanium* systems configured for console output to VGA, the **dom0** virtualized kernel may fail to boot. This is because the virtualized kernel failed to properly detect the default console device from the *Extensible Firmware Interface* (EFI) settings.

  When this occurs, add the boot parameter **console=tty** to the kernel boot options in **/boot/efi/elilo.conf**. (BZ#249076)
- On some *Itanium* systems (such as the *Hitachi Cold Fusion 3e*), the serial port cannot be detected in **dom0** when VGA is enabled by the EFI Maintenance Manager. As such, you need to supply the following serial port information to the **dom0** kernel:
  - Speed in bits/second
  - Number of data bits
  - Parity
  - **io_base** address

  These details must be specified in the **append=** line of the **dom0** kernel in **/boot/efi/elilo.conf**. For example:

  append="com1=19200,8n1,0x3f8 -- quiet rhgb console=tty0 console=ttyS0,19200n8"

  In this example, **com1** is the serial port, **19200** is the speed (in bits/second), **8n1** specifies the number of data bits/parity settings, and **0x3f8** is the **io_base** address. (BZ#433771)
- Virtualization does not work on some architectures that use Non-Uniform Memory Access (NUMA). As such, installing the virtualized kernel on systems that use NUMA will result in a boot failure.

  Some installation numbers install the virtualized kernel by default. If you have such an installation number and your system uses NUMA and does not work with kernel-xen, deselect the Virtualization option during installation.

2.15. kernel

The *kernel* packages contain the Linux kernel, the core of any Linux operating system.

- Starting with Red Hat Enterprise Linux 5.8, the size of I/O operations allowed by the NFS server has been increased by default. The new default max block size varies depending on RAM size, with a maximum of 1M (1048576 bytes).

  This may cause problems for 32-bit servers configured to use large numbers of **nfsd** threads. For such servers, we recommend decreasing the number of threads, or decreasing the I/O size by writing to the **/proc/fs/nfsd/max_block_size** file before starting **nfsd**. For example, the following command restores the previous default ***iosize*** of 32k:

  ```
  ~]# echo 32767 >/proc/fs/nfsd/max_block_size
  ```

  (BZ#765751)
- If the **qla4xxx** driver fails to discover all iSCSI targets, make sure to **Clear Persistent Targets** and set up iSCSI again via **CTRL+Q** in the Qlogic iSCSI optional BIOS.

- The OProfile infrastructure in Red Hat Enterprise Linux 5 does not support the hardware performance counters of the AMD family 0x15 processor family; profiling is only available in timer interrupt mode. When profiling on bare metal, OProfile automatically selects the timer interrupt mode. When running under kernel-xen, due to different CPU family reporting, OProfile must be explicitly configured to use timer interrupt mode. This is possible by adding **`options oprofile timer=1`** to the **`/etc/modprobe.conf`** file. (BZ#720587)
- Red Hat Enterprise Linux 5.8 may become unresponsive due to the lack of ticketed spinlocks in the **`shrink_active_list()`** function. As a result, the **`spin_lock_irq(&zone->lru_lock)`** operation disables interrupts, and the following error message is returned when the system hangs:

```
NMI Watchdog detected LOCKUP
```

- Booting a Red Hat Enterprise Linux 5.8 system with a connected DVD drive and the **`smartd`**service running hangs with the following error messages:

```
Starting smartd: hdc: drive_cmd: status=0x58 { DriveReady SeekComplete
DataRequest }
ide: failed opcode was: 0xa1
hdc: status error: status=0x58 { DriveReady SeekComplete DataRequest }
ide: failed opcode was: unknown
hdc: drive not ready for command
hdc: status timeout: status=0xd8 { Busy }
ide: failed opcode was: unknown
hdc: drive not ready for command
hdc: ATAPI reset complete
hdc: status error: status=0x58 { DriveReady SeekComplete DataRequest }
⋮
```

  To work around this issue, disconnect the DVD drive or turn the **`smartd`** service off with the following command:

```
~]# chkconfig smartd off
```

- The **`modify SRQ`** verb is not supported by the **`eHCA`** adapter and will fail with an error code when called from an application context.
- In RHEL 5.8, machine check (MCE) support for Intel Nehalem or newer CPUs (family 6, model >= 26) is disabled. This is a change from RHEL5.6 and earlier where basic MCE support was provided for these CPUs. Uncorrected CPU and memory errors will cause an immediate CPU shut down and system panic.
- On a Red Hat Enterprise Linux 5.8 system, while hand-loading the i386 (32-bit) kernel on z210/z210 SFF with BIOS 1.08, the system may fail to boot. To workaround this issue, please add the following parameter to the boot command line option:

```
pci=nosort
```

  (BZ#703538)
- Red Hat Enterprise Linux 5.7 has introduced a new multicast snooping feature for the bridge driver used for virtualization (virt-bridge). This feature is disabled by default in order to not break any existing configurations. To enable this feature, please set the following tunnable parameter to **1**:

```
/sys/class/net/breth0/bridge/multicast_snooping
```

  Please note that when multicast snooping is enabled, it may cause a regression with certain

switches where it causes a break in the multicast forwarding for some peers.

- By default, **libsas** defines a wideport based on the attached SAS address, rather than the specification compliant “strict” definition of also considering the local SAS address. In Red Hat Enterprise Linux 5.8, only the default “loose” definition is available. The implication is that if an OEM configures an SCU controller to advertise different SAS addresses per PHY, but hooks up a wide target or an expander to those PHYs, libsas will only create one port. The expectation, in the “strict” case, is that this would result in a single controller multipath configuration.

  It is not possible to use a single controller multipath without the **strict_wide_port** functionality. Multi-controller multipath should behave as a expected.

  A x8 multipath configuration through a single expander can still be obtained under the following conditions:

  1. Start with an SCU SKU that exposes (2) x4 controllers (total of 8 PHYs)
  2. Assign ***sas_address1*** to all the PHYs on **controller1**
  3. Assign ***sas_address2*** to all the PHYs on **controller2**
  4. Hook up the expander across all 8 PHYs
  5. Configure multipath across the two controller instances

  It is critical for **controller1** to have a distinct address from **controller2**, otherwise the expander will be unable to correctly route connection requests to the proper initiator. (BZ#651837)
- On a Red Hat Enterprise Linux 5.8 system, it is advisable to update the firmware of the HP ProLiant Generation 6 (G6) controller's firmware to version 5.02 or later. Once the firmware is successfully updated, reboot the system and Kdump will work as expected.

  HP G6 controllers include: P410i, P411, P212, P712, and P812

  In addition, kdump may fail when using the HP Smart Array 5i Controller on a Red Hat Enterprise Linux 5.8 system. (BZ#695493)
- On Red Hat Enterprise Linux 5.5 and later, suspending the system with the **lpfc** driver loaded may crash the system during the resume operation. Therefore, systems using the **lpfc** driver, either unload the **lpfc** driver before the system is suspended, or ,if that is not possible, do not suspend the system. (BZ#703631)
- NUMA class systems should not be booted with a single memory node configuration. Configuration of single node NUMA systems will result in contention for the memory resources on all of the non-local memory nodes. As only one node will have local memory the CPUs on that single node will starve the remaining CPUs for memory allocations, locks, and any kernel data structure access. This contention will lead to the "CPU#n stuck for 10s!" error messages. This configuration can also result in NMI watchdog timeout panics if a spinlock is acquired via **spinlock_irq()** and held for more than 60 seconds. The system can also hang for indeterminate lengths of time.

  To minimize this problem, NUMA class systems need to have their memory evenly distributed between nodes. NUMA information can be obtained from dmesg output as well as from the **numastat** command. (BZ#529428)
- When upgrading from Red Hat Enterprise Linux 5.0, 5.1 or 5.2 to more recent releases, the gfs2-kmod may still be installed on the system. This package must be manually removed or it will override the (newer) version of GFS2 which is built into the kernel. Do not install the **gfs2-kmod** package on later versions of Red Hat Enterprise Linux. **gfs2-kmod** is not required since GFS2 is built into the kernel from 5.3 onwards. The content of the gfs2-kmod package is considered a Technology Preview of GFS2, and has not received any updates since Red Hat Enterprise Linux 5.3 was released.

  Note that this note only applies to GFS2 and not to GFS, for which the gfs-kmod package continues to be the only method of obtaining the required kernel module.
- Issues might be encountered on a system with 8Gb/s LPe1200x HBAs and firmware version 2.00a3 when the Red Hat Enterprise Linux 5.8 kernel is used with the in-box LPFC driver. Such issues include loss of LUNs and/or fiber channel host hangs during fabric faults with multipathing.

To work around these issues, it is recommended to either:

- Downgrade the firmware revision of the 8Gb/s LPe1200x HBA to revision 1.11a5, or
- Modify the LPFC driver's **lpfc_enable_npiv** module parameter to zero.

  When loading the LPFC driver from the initrd image (i.e. at system boot time), add the line

  ```
  options lpfc_enable_npiv=0
  ```

  to **/etc/modprobe.conf** and re-build the initrd image.

  When loading the LPFC driver dynamically, include the **lpfc_enable_npiv=0** option in the insmod or modprobe command line.

For additional information on how to set the LPFC driver module parameters, refer to the Emulex Drivers for Linux User Manual.

- If AMD IOMMU is enabled in BIOS on ProLiant DL165 G7 systems, the system will reboot automatically when IOMMU attempts to initialize. To work around this issue, either disable IOMMU, or update the BIOS to version **2010.09.06** or later. (BZ#628534)
- As of Red Hat Enterprise Linux 5.6, the **ext4** file system is fully supported. However, provisioning ext4 file systems with the anaconda installer is not supported, and ext4 file systems need to be provisioned manually after the installation. (BZ#563943)
- In some cases the NFS server fails to notify NFSv4 clients about renames and unlinks done by other clients, or by non-NFS users of the server. An application on a client may then be able to open the file at its old pathname (and read old cached data from it, and perform read locks on it), long after the file no longer exists at that pathname on the server.

  To work around this issue, use NFSv3 instead of NFSv4. Alternatively, turn off support for leases by writing ***0*** to **/proc/sys/fs/leases-enable** (ideally on boot, before the nfs server is started). This change prevents NFSv4 delegations from being given out, restore correctness at the expense of some performance.
- Some laptops may generate continuous events in response to the lid being shut. Consequently, the gnome-power-manager utility will consume CPU resources as it responds to each event. (BZ#660644)
- A kernel panic may be triggered by the lpfc driver when multiple Emulex OneConnect Universal Converged Network Adapter initiators are included in the same Storage Area Network (SAN) zone. Typically, this kernel panic will present after a cable is pulled or one of the systems is rebooted. To work around this issue, configure the SAN to use single initiator zoning. (BZ#574858)
- If a Huawei USB modem is unplugged from a system, the device may not be detected when it is attached again. To work around this issue, the usbserial and usb-storage driver modules need to be reloaded, allowing the system to detect the device. Alternatively, the if the system is rebooted, the modem will be detected also. (BZ#517454)
- Memory on-line is not currently supported with the Boxboro-EX platform. (BZ#515299)
- Unloading a PF (SR-IOV Physical function) driver from a host when a guest is using a VF (virtual function) from that device can cause a host crash. A PF driver for an SR-IOV device should not be unloaded until after all guest virtual machines with assigned VFs from that SR-IOV device have terminated. (BZ#514360)
- Data corruption on NFS file systems might be encountered on network adapters without support for error-correcting code (ECC) memory that also have TCP segmentation offloading (TSO) enabled in the driver. Note: data that might be corrupted by the sender still passes the checksum performed by the IP stack of the receiving machine A possible work around to this issue is to disable TSO on network adapters that do not support ECC memory. (BZ#504811)
- After installation, a System z machine with a large number of memory and CPUs (e.g. 16 CPU's and 200GB of memory) might may fail to IPL. To work around this issue, change the line

```
ramdisk=/boot/initrd-2.6.18-<kernel-version-number>.el5.img
```

to

```
ramdisk=/boot/initrd-2.6.18-<kernel-version-number>.el5.img,0x02000000
```

The command **zipl -V** should now show **0x02000000** as the starting address for the initial RAM disk (initrd). Stop the logical partition (LPAR), and then manually increase the storage size of the LPAR.

- On certain hardware configurations the kernel may panic when the Broadcom iSCSI offload driver (**bnx2i.ko** and **cnic.ko**) is loaded. To work around this do not manually load the bnx2i or cnic modules, and temporarily disable the **iscsi** service from starting. To disable the iscsi service, run:

```
~]# chkconfig --del iscsi
~]# chkconfig --del iscsid
```

On the first boot of your system, the **iscsi** service may start automatically. To bypass this, during bootup, enter interactive start up and stop the iscsi service from starting.

- In Red Hat Enterprise Linux 5, invoking the kernel system call "setpriority()" with a "which" parameter of type "PRIO_PROCESS" does not set the priority of child threads. (BZ#472251)
- A change to the cciss driver in Red Hat Enterprise Linux 5.4 made it incompatible with the **echo disk < /sys/power/state** suspend-to-disk operation. Consequently, the system will not suspend properly, returning messages such as:

```
Stopping tasks:
=======================================================================
stopping tasks timed out after 20 seconds (1 tasks remaining):
cciss_scan00
Restarting tasks...<6> Strange, cciss_scan00 not stopped
done
```

(BZ#513472)

- The kernel is unable to properly detect whether there is media present in a CD-ROM drive during kickstart installs. The function to check the presence of media incorrectly interprets the "logical unit is becoming ready" sense, returning that the drive is ready when it is not. To work around this issue, wait several seconds between inserting a CD and asking the installer (anaconda) to refresh the CD. (BZ#510632)
- When a cciss device is under high I/O load, the kdump kernel may panic and the vmcore dump may not be saved successfully. (BZ#509790)
- Configuring IRQ SMP affinity has no effect on some devices that use message signaled interrupts (MSI) with no MSI per-vector masking capability. Examples of such devices include *Broadcom NetXtreme* Ethernet devices that use the **bnx2** driver.

  If you need to configure IRQ affinity for such a device, disable MSI by creating a file in **/etc/modprobe.d/** containing the following line:

```
options bnx2 disable_msi=1
```

  Alternatively, you can disable MSI completely using the kernel boot parameter **pci=nomsi**. (BZ#432451)
- The **smartctl** tool cannot properly read SMART parameters from SATA devices. (BZ#429606)
- *IBM T60* laptops will power off completely when suspended and plugged into a docking station. To

avoid this, boot the system with the argument **acpi_sleep=s3_bios**. (BZ#439006)

- The *QLogic iSCSI Expansion Card* for the *IBM Bladecenter* provides both ethernet and iSCSI functions. Some parts on the card are shared by both functions. However, the current **qla3xxx** and **qla4xxx** drivers support ethernet and iSCSI functions individually. Both drivers do not support the use of ethernet and iSCSI functions simultaneously.

  Because of this limitation, successive resets (via consecutive **ifdown**/**ifup** commands) may hang the device. To avoid this, allow a 10-second interval after an **ifup** before issuing an **ifdown**. Also, allow the same 10-second interval after an **ifdown** before issuing an **ifup**. This interval allows ample time to stabilize and re-initialize all functions when an **ifup** is issued. (BZ#276891)

- Laptops equipped with the *Cisco Aironet MPI-350* wireless may hang trying to get a DHCP address during any network-based installation using the wired ethernet port.

  To work around this, use local media for your installation. Alternatively, you can disable the wireless card in the laptop BIOS prior to installation (you can re-enable the wireless card after completing the installation). (BZ#213262)

- Hardware testing for the *Mellanox MT25204* has revealed that an internal error occurs under certain high-load conditions. When the **ib_mthca** driver reports a catastrophic error on this hardware, it is usually related to an insufficient completion queue depth relative to the number of outstanding work requests generated by the user application.

  Although the driver will reset the hardware and recover from such an event, all existing connections at the time of the error will be lost. This generally results in a segmentation fault in the user application. Further, if **opensm** is running at the time the error occurs, then you need to manually restart it in order to resume proper operation. (BZ#251934)

- The *IBM T41* laptop model does not enter **Suspend Mode** properly; as such, **Suspend Mode** will still consume battery life as normal. This is because Red Hat Enterprise Linux 5 does not yet include the **radeonfb** module.

  To work around this, add a script named **hal-system-power-suspend** to **/usr/share/hal/scripts/** containing the following lines:

  ```
  chvt 1
  radeontool light off
  radeontool dac off
  ```

  This script will ensure that the *IBM T41* laptop enters **Suspend Mode** properly. To ensure that the system resumes normal operations properly, add the script **restore-after-standby** to the same directory as well, containing the following lines:

  ```
  radeontool dac on
  radeontool light on
  chvt 7
  ```

  (BZ#227496)

- If the **edac** module is loaded, BIOS memory reporting will not work. This is because the **edac** module clears the register that the BIOS uses for reporting memory errors.

  The current Red Hat Enterprise Linux Driver Update Model instructs the kernel to load all available modules (including the **edac** module) by default. If you wish to ensure BIOS memory reporting on your system, you need to manually blacklist the **edac** modules. To do so, add the following lines to **/etc/modprobe.conf**:

```
blacklist edac_mc
blacklist i5000_edac
blacklist i3000_edac
blacklist e752x_edac
```

(BZ#441329)

- Due to outstanding driver issues with hardware encryption acceleration, users of Intel WiFi Link 4965, 5100, 5150, 5300, and 5350 wireless cards are advised to disable hardware accelerated encryption using module parameters. Failure to do so may result in the inability to connect to Wired Equivalent Privacy (WEP) protected wireless networks after connecting to WiFi Protected Access (WPA) protected wireless networks.

  To do so, add the following options to **/etc/modprobe.conf**:

  ```
  alias wlan0 iwlagn
  options iwlagn swcrypto50=1 swcrypto=1
  ```

  where wlan0 is the default interface name of the first Intel WiFi Link device.

  (BZ#468967)

- A kernel security fix released between Red Hat Enterprise Linux 5.7 and 5.8 may prevent PCI passthrough working and guests starting. Refer to Red Hat Knowledgebase article 66747 for further details.

The following note applies to the PowerPC architecture:

- The size of the PowerPC kernel image is too large for OpenFirmware to support. Consequently, network booting will fail, resulting in the following error message:

  ```
  Please wait, loading kernel...
  /pci@8000000f8000000/ide@4,1/disk@0:2,vmlinux-anaconda: No such file or
  directory
  boot:
  ```

  To work around this:

  1. Boot to the OpenFirmware prompt, by pressing the '8' key when the IBM splash screen is displayed.
  2. Run the following command:

     ```
     ~]# setenv real-base 2000000
     ```

  3. Boot into System Management Services (SMS) with the command:

     ```
     ~]# 0> dev /packages/gui obe
     ```

  (BZ#462663)

2.16. kexec-tools

The *kexec-tools* package provides the **/sbin/kexec** binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot.

- Executing **kdump** on an *IBM Bladecenter QS21* or *QS22* configured with NFS root will fail. To avoid this, specify an NFS dump target in **/etc/kdump.conf**. (BZ#368981)
- Some **forcedeth** based devices may encounter difficulty accessing memory above 4GB during

operation in a **kdump** kernel. To work around this issue, add the following line to the **/etc/sysconfig/kdump** file:

```
KDUMP_COMMANDLINE_APPEND="dma_64bit=0"
```

This work around prevents the **forcedeth** network driver from using high memory resources in the kdump kernel, allowing the network to function properly.

- The system may not successfully reboot into a **kexec**/**kdump** kernel if X is running and using a driver other than *vesa*. This problem only exists with *ATI Rage XL* graphics chipsets.

  If X is running on a system equipped with *ATI Rage XL*, ensure that it is using the *vesa* driver in order to successfully reboot into a **kexec**/**kdump** kernel. (BZ#221656)
- **kdump** now serializes drive creation registration with the rest of the **kdump** process. Consequently, **kdump** may hang waiting for IDE drives to be initialized. In these cases, it is recommended that IDE disks not be used with **kdump**. (BZ#473852)
- It is possible in rare circumstances, for **makedumpfile** to produce erroneous results but not have them reported. This is due to the fact that **makedumpfile** processes its output data through a pipeline consisting of several stages. If **makedumpfile** fails, the other stages will still succeed, effectively masking the failure. Should a vmcore appear corrupt, and makedumpfile is in use, it is recommended that the core be recorded without makedumpfile and a bug be reported. (BZ#475487)
- kdump now restarts when CPUs or DIMMs are hot-added to a system. If multiple items are added at the same time, several sequential restarts may be encountered. This behavior is intentional, as it minimizes the time-frame where a crash may occur while memory or processors are not being tracked by kdump. (BZ#474409)

The following known issue applies to the Itanium architecture:

- Some *Itanium* systems cannot properly produce console output from the **kexec purgatory** code. This code contains instructions for backing up the first 640k of memory after a crash.

  While **purgatory** console output can be useful in diagnosing problems, it is not needed for **kdump** to properly function. As such, if your *Itanium* system resets during a **kdump** operation, disable console output in **purgatory** by adding **--noio** to the **KEXEC_ARGS** variable in **/etc/sysconfig/kdump**. (BZ#436426)

2.17. kvm

Kernel-based Virtual Machine (KVM) is a full virtualization solution for Linux on x86 hardware.

KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel. KVM can run multiple unmodified, virtualized guest Windows and Linux operating systems. KVM is a hypervisor which uses the libvirt virtualization tools (virt-manager and virsh).

- Erroneous boot-index of a guest with mixed virtio/IDE disks causes the guest to boot from the wrong disk after the OS installation and hang with the error message **boot from HD**.
- When using PCI device assignment with a 32-bit Microsoft Windows 2008 guest on an AMD-based host system, the assigned device may fail to work properly if it relies on MSI or MSI-X based interrupts. The reason for this is that the 32-bit version of Microsoft Windows 2008 does not enable MSI based interrupts for the family of processor exposed to the guest. To work around this problem, the user may wish to move to a RHEL6 host, use a 64-bit version of the guest operating system, or employ a wrapper script to modify the processor family exposed to the guest as follows (Note that this is only for 32-bit Windows guests):
  1. Create the following wrapper script:

```
~]$ cat /usr/libexec/qemu-kvm.family16
#!/bin/sh

ARGS=$@

echo $ARGS | grep -q ' -cpu '
if [ $? -eq 0 ]; then
    for model in $(/usr/libexec/qemu-kvm -cpu ? \
                    | sed 's|^x86||g' | tr -d [:blank:]); do
        ARGS=$(echo $ARGS | \
                sed "s|-cpu $model|-cpu $model,family=16|g")
    done
else
    ARGS="$ARGS -cpu qemu64,family=16"
fi

echo "$0: exec /usr/libexec/qemu-kvm $ARGS" >&2

exec /usr/libexec/qemu-kvm $ARGS
```

2. Make the script executable:

```
~]$ chmod 755 /usr/libexec/qemu-kvm.family16
```

3. Set proper SELinux permissions:

```
~]$ restorecon /usr/libexec/qemu-kvm.family16
```

4. Update the guest XML to use the new wrapper:

```
~]# virsh edit $GUEST
```

and replace:

```
<emulator>/usr/libexec/qemu-kvm</emulator>
```

with:

```
<emulator>/usr/libexec/qemu-kvm.family16</emulator>
```

(BZ#654208)

- Booting a Linux guest causes 1.5 to 2 second time drift from the host time when the default **hwclock** service starts. It is recommended to disable the hwclock service. Alternatively, enable the **ntp** service so that it can correct the time once the service is started. (BZ#523478)
- By default, KVM virtual machines created in Red Hat Enterprise Linux 5.6 have a virtual Realtek 8139 (rtl8139) network interface controller (NIC). The rtl8139 virtual NIC works fine in most environments, but may suffer from performance degradation issues on some networks for example, a 10 GigE (10 Gigabit Ethernet) network.

  One workaround for this issue is switch to a different type of virtual NIC, for example, Intel PRO/1000 (e1000) or virtio (a virtual I/O driver for Linux that can talk to the hypervisor).

  To switch to e1000:

  1. Shutdown the guest OS
  2. Edit the guest OS definition with the command-line tool virsh:

```
virsh edit GUEST
```

3. Locate the network interface section and add a model line as shown:

```
<interface type='network'>
...
<model type='e1000' />
</interface>
```

4. Save the changes and exit the text editor
5. Restart the guest OS

Alternatively, if you're having trouble installing the OS on the virtual machine because of the rtl8139 NIC (for example, because you're installing the OS over the network), you can create a virtual machine from scratch with an e1000 NIC. This method requires you to have at least one virtual machine already created (possibly installed from CD or DVD) to use as a template.

1. Create an XML template from an existing virtual machine:

```
virsh dumpxml GUEST > /tmp/guest.xml
```

2. Copy and edit the XML file and update the unique fields: virtual machine name, UUID, disk image, MAC address, etc. Note that you can delete the UUID and MAC address lines and virsh will generate a UUID and MAC address.

```
cp /tmp/guest.xml /tmp/new-guest.xml
vi /tmp/new-guest.xml
```

3. Locate the network interface section and add a model line as shown:

```
<interface type='network'>
...
<model type='e1000' />
</interface>
```

4. Create the new virtual machine:

```
virsh define /tmp/new-guest.xml
virsh start new-guest
```

- The mute button in the audio control panel on a Windows virtual machine does not mute the sound.
- When migrating KVM guests between hosts, the NX CPU feature setting on both source and destination must match. Migrating a guest between a host with the NX feature disabled (i.e. disabled in the BIOS settings) and a host with the NX feature enabled may cause the guest to crash. (BZ#516029)
- The use of the qcow2 disk image format with KVM is considered a Technology Preview. (BZ#517880)
- 64-bit versions of Windows 7 do not have support for the AC'97 Audio Codec. Consequently, the virtualized sound device Windows 7 kvm guests will not function. (BZ#563122)
- Hot plugging emulated devices after migration may result in the virtual machine crashing after a reboot or the devices no longer being visible. (BZ#507191)
- The KVM modules from the **kmod-kvm** package do not support kernels prior to version 2.6.18-203.el5. If kmod-kvm is updated and an older kernel is kept installed, error messages similar to the following will be returned if attempting to install these modules on older kernels:

```
WARNING: /lib/modules/2.6.18-194.el5/weak-updates/kmod-kvm/ksm.ko needs unknown
symbol kvm_ksm_spte_count
```

(BZ#509361)

- The KVM modules available in the **kmod-kvm** package are loaded automatically at boot time if the kmod-kvm package is installed. To make these KVM modules available after installing the **kmod-kvm** package the system either needs to be rebooted or the modules can be loaded manually by running the **/etc/sysconfig/modules/kvm.modules** script. (BZ#501543)
- The Preboot eXecution Environment (PXE) boot ROMs included with KVM are from the Etherboot project. Consequently, some bug fixes or features that are present on the newer gPXE project are not available on Etherboot. For example, Virtual Machines (VMs) cannot boot using Microsoft based PXE (that is, Remote Installation Services (RIS) or Windows Deployment Services (WDS)).
- The following QEMU / KVM features are currently disabled and not supported: (BZ#512837)
  - smb user directories
  - scsi emulation
  - "isapc" machine type
  - nested KVM guests
  - usb mass storage device emulation
  - usb wacom tablet emulation
  - usb serial emulation
  - usb network emulation
  - usb bluetooth emulation
  - device emulation for vmware drivers
  - sb16 and es1370 sound card emulations
  - bluetooth emulation
  - qemu CPU models other than qemu32/64 and pentium3
  - qemu block device drivers other than raw, qcow2, and host_device

2.18. less

The less utility is a text file browser that resembles more, but with more capabilities ("less is more"). The less utility allows users to move backwards in the file as well as forwards. Because less need not read the entire input file before it starts, less starts up more quickly than text editors (vi, for example).

- The "less" command has been updated. less no longer adds the "carriage return" character when wrapping long lines. Consequently, lines longer than the terminal width will be displayed incorrectly when browsing the file line per line. The command line option "--old-bot" forces less to behave as it did previously, with long text lines displayed correctly. (BZ#441691)

2.19. lftp

LFTP is a sophisticated file transfer program for the FTP and HTTP protocols. Like bash, it has job control and uses the readline library for input. It has bookmarks, built-in mirroring, and can transfer several files in parallel. It is designed with reliability in mind.

- As a side effect of changing the underlying cryptographic library from OpenSSL to GnuTLS in the past, starting with *lftp-3.7.11-4.el5_5.3*, some previously offered TLS ciphers were dropped. In handshake, **lftp** does not offer these previously available ciphers:

```
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_DES_CBC_SHA
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
```

lftp still offers variety of other TLS ciphers:

```
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_DHE_DSS_WITH_RC4_128_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
```

For servers without support for any of these ciphers, it is now possible to force SSLv3 connection instead of TLS using the **`set ftp:ssl-auth SSL`** configuration directive. This works both for implicit and explicit FTPS. (BZ#532099)

2.20. lvm2

The lvm2 package contains support for Logical Volume Management (LVM).

- LVM no longer scans multipath member devices (underlying paths for active multipath devices) and prefers top level devices. This behavior can be switched off using the **`multipath_component_detection`** option in the **`/etc/lvm/lvm.conf`**.

2.21. mesa

Mesa provides a 3D graphics API that is compatible with OpenGL. It also provides hardware-accelerated drivers for many popular graphics chips.

The following known issue applies to the Intel 64 and AMD64 architectures:

- On an *IBM T61* laptop, Red Hat recommends that you refrain from clicking the **`glxgears`** window (when **`glxgears`** is run). Doing so can lock the system.

  To prevent this from occurring, disable the tiling feature. To do so, add the following line in the **`Device`** section of **`/etc/X11/xorg.conf`**:

  ```
  Option "Tiling" "0"
  ```

  (BZ#444508)

2.22. mkinitrd

The mkinitrd utility creates file system images for use as initial RAM disk (initrd) images.

- When using an encrypted device, the following error message may be reported during bootup:

```
insmod: error inserting '/lib/aes_generic.ko': -1 File exists
```

  This message can safely be ignored. (BZ#466296)
- Installation using a Multiple Device (MD) RAID on top of multipath will result in a machine that cannot boot. Multipath to Storage Area Network (SAN) devices which provide RAID internally are not affected. (BZ#467469)

The following known issue applies to the IBM System z architecture:

- When installing Red Hat Enterprise Linux 5.8, the following errors may be returned in **install.log**:

```
Installing kernel-2.6.18-158.el5.s390x
cp: cannot stat `/sbin/dmraid.static': No such file or directory
```

  This message can be safely ignored.
- iSCSI root devices do not function correctly if used over an IPv6 network connection. While the installation will appear to succeed, the system will fail to find the root file system during the first boot. (BZ#529636)

2.23. mod_revocator

The mod_revocator module retrieves and installs remote Certificate Revocation Lists (CRLs) into an Apache web server.

- In order to run **mod_revocator** successfully, the following command must be executed in order to allow **httpd** to connect to a remote port which SELinux would otherwise deny:

```
~]# setsebool -P httpd_can_network_connect=1
```

  This is due to the fact that by default, Apache is not allowed to also be used as an HTTP client (that is, send HTTP messages to an external host).

2.24. openib

The OpenFabrics Alliance Enterprise Distribution (OFED) is a collection of Infiniband and iWARP hardware diagnostic utilities, the Infiniband fabric management daemon, Infiniband/iWARP kernel module loader, and libraries and development packages for writing applications that use Remote Direct Memory Access (RDMA) technology. Red Hat Enterprise Linux uses the OFED software stack as its complete stack for Infiniband/iWARP/RDMA hardware support.

The following known issue applies to the Itanium architecture:

- Running **perftest** will fail if different CPU speeds are detected. As such, you should disable CPU speed scaling before running **perftest**. (BZ#433659)

2.25. openmpi

Open MPI, MVAPICH, and MVAPICH2 are all competing implementations of the Message Passing Interface (MPI) standard. MVAPICH implements version 1 of the MPI standard, while Open MPI and

MVAPICH2 both implement the later, version 2 of the MPI standard.

- **mvapich** and **mvapich2** in Red Hat Enterprise Linux 5 are compiled to support only *InfiniBand/iWARP* interconnects. Consequently, they will not run over ethernet or other network interconnects. (BZ#466390)
- When upgrading openmpi using yum, the following warning may be returned:

  ```
  cannot open `/tmp/openmpi-upgrade-version.*' for reading: No such file or
  directory
  ```

  The message is harmless and can be safely ignored. (BZ#463919)
- A bug in previous versions of **openmpi** and **lam** may prevent you from upgrading these packages. This bug manifests in the following error (when attempting to upgrade **openmpi** or **lam**:

  ```
  error: %preun(openmpi-[version]) scriptlet failed, exit status 2
  ```

  As such, you need to manually remove older versions of **openmpi** and **lam** in order to install their latest versions. To do so, use the following **rpm** command:

  ```
  rpm -qa | grep '^openmpi-\|^lam-' | xargs rpm -e --noscripts --allmatches
  ```

  (BZ#433841)

2.26. perl-libxml-enno

The perl-libxml-enno modules were used for XML parsing and validation.

- Note: the perl-libxml-enno library did not ship in any Red Hat Enterprise Linux 5 release. (BZ#612589)

2.27. pm-utils

The *pm-utils* package contains utilities and scripts for power management.

- nVidia video devices on laptops can not be correctly re-initialized using VESA in Red Hat Enterprise Linux 5. Attempting to do so results in a black laptop screen after resume from suspend.

2.28. rpm

The RPM Package Manager (RPM) is a command line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.

- Users of a freshly-installed PowerPC Red Hat Enterprise Linux 5.8 system may encounter package-related operation failures with the following errors:

  ```
  rpmdb: PANIC: fatal region error detected; run recovery
  error: db4 error(-30977) from db->sync: DB_RUNRECOVERY: Fatal error, run
  database recovery
  ```

2.29. redhat-release-notes

The *redhat-release-notes* package contains the Release Notes for Red Hat Enterprise Linux 5.8.

- The Revision History of the Red Hat Enterprise Linux 5.8 Release Notes contains an incorrect release date for the **1-0** revision: **Thu Feb 16 2011**. The revision date should be **Tue Feb 21 2012**. The content of the Release Notes reflects changes made to Red Hat Enterprise Linux 5.8.

2.30. qspice

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display system built for virtual environments which allows users to view a computing 'desktop' environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures.

- Occasionally, the video compression algorithm starts when the guest is accessing text instead of video. This caused the text to be blurred. The SPICE server now has an improved heuristic for distinguishing between videos and textual streams.

2.31. subscription-manager

The new Subscription Management tooling allows users to understand the specific products which have been installed on their machines, and the specific subscriptions which their machines are consuming.

- Using Subscription Manager in the following use case fails: a user installs Red Hat Enterprise Linux Desktop from a Red Hat Enterprise Linux 5.7 Client CD/DVD without an installation number. A user uses Subscription Manager, which finds one Red Hat Enterprise Linux Desktop product ID to subscribe to a Red Hat Enterprise Linux Workstation subscription. A user downloads content from a Workstation repository.

  The use case scenario described above fails because the rhel-workstation repositories require the rhel-5-workstation product tag in the product certification beforehand in order to view them.

  To work around this issue, follow these steps:

  1. Install a rhel-5-client system.
  2. Mount the ISO to your file system.
  3. Copy ***<path_to_ISO>*/Workstation/repodata/productid** to the **/etc/pki/product/** directory, making sure that the file copied ends with **.pem** (for example, **/etc/pki/product/productid.pem**)
  4. Subscribe to a Workstation subscription.
  5. Install a package from a Workstation repository.

2.32. systemtap

SystemTap provides an instrumentation infrastructure for systems running the Linux 2.6 kernel. It allows users to write scripts that probe and trace system events for monitoring and profiling purposes. SystemTap's framework allows users to investigate and monitor a wide variety of wide variety of kernel functions, system calls, and other evens that occur in both kernel-space and user-space.

- Running some user-space probe test cases provided by the **systemtap-testsuite** package fail with an **Unknown symbol in module** error on some architectures. These test cases include (but are not limited to):
  - **systemtap.base/uprobes.exp**
  - **systemtap.base/bz10078.exp**
  - **systemtap.base/bz6850.exp**

- **systemtap.base/bz5274.exp**

  Because of a known bug in the latest SystemTap update, new SystemTap installations do not unload old versions of the **uprobes.ko** module. Some updated user-space probe tests provided by the systemtap-testsuite package use symbols available only in the latest **uprobes.ko** module (also provided by the latest SystemTap update). As such, running these user-space probe tests result in the error mentioned earlier.

  If you encounter this error, simply run **rmmod uprobes** to manually remove the older **uprobes.ko** module before running the user-space probe test again. (BZ#499677)

- SystemTap currently uses GCC to probe user-space events. GCC is, however, unable to provide debuggers with precise location list information for parameters. In some cases, GCC also fails to provide visibility on some parameters. As a consequence, SystemTap scripts that probe user-space may return inaccurate readings. (BZ#239065)

2.33. xen

- In some cases, Red Hat Enterprise Linux 6 guests running fully-virtualized under Red Hat Enterprise Linux 5 experience a time drift or fail to boot. In some cases, drifting may start after migration of the virtual machine to a host with different speed. This is due to limitations in the Red Hat Enterprise Linux 5 Xen Hypervisor. To work around this, add **clocksource=acpi_pm** or **clocksource=jiffies** to the kernel command line for the guest. Alternatively, if running under Red Hat Enterprise Linux 5.7 or newer, locate the guest configuration file for the guest and add the **hpet=0** option in it.
- There are only 2 virtual slots (00:06.0 and 00:07.0) that are available for hot plug support in a virtual guest. (BZ#564261)
- As of Red Hat Enterprise Linux 5.4, PCI devices connected to a single PCI-PCI bridge can no longer be assigned to different PV guests. If the old, unsafe behavior is required, disable pci-dev-assign-strict-check in /etc/xen/xend-config.sxp. (BZ#508310)
- When running x86_64 Xen, it is recommended to set dom0-min-mem in /etc/xen/xend-config.sxp to a value of 1024 or higher. Lower values may cause the dom0 to run out of memory, resulting in poor performance or out-of-memory situations. (BZ#519492)
- The Red Hat Enterprise Linux 3 kernel does not include SWIOTLB support. SWIOTLB support is required for Red Hat Enterprise Linux 3 guests to support more than 4GB of memory on AMD Opteron and Athlon-64 processors. Consequently, Red Hat Enterprise Linux 3 guests are limited to 4GB of memory on AMD processors. (BZ#504187)
- The Hypervisor outputs messages regarding attempts by any guest to write to an MSR. Such messages contain the statement **Domain attempted WRMSR**. These messages can be safely ignored; furthermore, they are rate limited and should pose no performance risk. (BZ#477647)

The following known issues applies to the Intel 64 and AMD64 architectures:

- Installing Red Hat Enterprise Linux 3.9 on a fully virtualized guest may be extremely slow. In addition, booting up the guest after installation may result in **hda: lost interrupt** errors.

  To avoid this bootup error, configure the guest to use the SMP kernel. (BZ#249521)

2.34. virt-v2v

The virt-v2v package provides a tool for converting virtual machines to use the KVM hypervisor or Red Hat Enterprise Virtualization. The tool can import a variety of guest operating systems from libvirt-managed hosts and VMware ESX.

- **VMware Tools** on Microsoft Windows is unable to disable itself when it detects that it is no longer running on a VMware platform. As a consequence, converting a Microsoft Windows guest from VMware ESX, which has **VMware Tools** installed, resulted in multiple error messages being displayed on startup. In addition, a **Stop Error** (also known as Blue Screen of Death, or BSOD) was displayed every time when shutting down the guest. To work around this issue, users are advised to uninstall VMware Tools from Microsoft Windows guests before conversion. (BZ#711972)

2.35. virtio-win

VirtIO para-virtualized Windows(R) drivers for 32-bit and 64-bit Windows (R) guests.

- Low performance with UDP messages larger than 1024 is a known Microsoft issue: http://support.microsoft.com/default.aspx/kb/235257. For the message larger than 1024 bytes follow the workaround procedure detailed in the above Microsoft knowledgebase article.
- Installation of Windows XP with the floppy containing guest drivers (in order to get the virtio-net drivers installed as part of the installation), will return messages stating that the viostor.sys file could not be found. viostor.sys is not part of the network drivers, but is on the same floppy as portions of the virtio-blk drivers. These messages can be safely ignored, simply accept the installation's offer to reboot, and the installation will continue normally.

2.36. xorg-x11-drv-i810

xorg-x11-drv-i810 is an Intel integrated graphics video driver for the X.Org implementation of the X Window System.

- When switching from the X server to a virtual terminal (VT) on a Lenovo ThinkPad T510 laptop, the screen may remain blank. Switching back to the X server will restore the screen.
- Running a screensaver or resuming a suspended laptop with an external monitor attached may result in a blank screen or a brief flash followed by a blank screen. If this occurs with the screensaver, the prompt for your password is being obscured, the password can still be entered blindly to get back to the desktop. To work around this issue, physically disconnect the external monitor and then press the video hotkey (usually Fn-F7) to rescan the available outputs, before suspending the laptop.

The following known issues apply to the Intel 64 and AMD64 architectures:

- If your system uses an *Intel 945GM* graphics card, do not use the **i810** driver. You should use the default **intel** driver instead. (BZ#468218)
- On dual-GPU laptops, if one of the graphics chips is Intel-based, the Intel graphics mode cannot drive any external digital connections (including HDMI, DVI, and DisplayPort). This is a hardware limitation of the Intel GPU. If you require external digital connections, configure the system to use the discrete graphics chip (in the BIOS). (BZ#468259)

2.37. xorg-x11-drv-nv

xorg-x11-drv-nv provides a driver for NVIDIA cards for the X.org implementation of the X Window System.

- Improvements have been made to the 'nv' driver, enhancing suspend and resume support on some systems equipped with nVidia GeForce 8000 and 9000 series devices. Due to technical limitations, this will not enable suspend/resume on all hardware. (BZ#414971)

The following known issue applies to the Intel 64 and AMD64 architectures:

- Some machines that use *NVIDIA* graphics cards may display corrupted graphics or fonts when using the graphical installer or during a graphical login. To work around this, switch to a virtual console and back to the original X host. (BZ#222737, BZ#221789)

2.38. xorg-x11-drv-vesa

xorg-x11-drv-vesa is a video driver for the X.Org implementation of the X Window System. It is used as a fallback driver for cards with no native driver, or when the native driver does not work.

The following known issue applies to the x86 architecture:

- When running the bare-metal (non-Virtualized) kernel, the X server may not be able to retrieve **`EDID`** information from the monitor. When this occurs, the graphics driver will be unable to display resolutions highers than 800x600.

  To work around this, add the following line to the **`ServerLayout`** section of **`/etc/X11/xorg.conf`**:

  ```
  Option "Int10Backend" "x86emu"
  ```

  (BZ#236416)

2.39. yaboot

The *yaboot* package is a boot loader for Open Firmware based PowerPC systems. It can be used to boot IBM eServer System p machines.

- If the string that represents the path to kernel (or ramdisk) is greater than 63 characters, network booting an IBM POWER5 series system may result in the following error:

  ```
  FINAL File Size = 8948021 bytes.
  load-base=0x4000
  real-base=0xc00000
  DEFAULT CATCH!, exception-handler=fff00300
  ```

  The firmware for IBM POWER6 and IBM POWER7 systems contains a fix for this issue. (BZ#550086)

Chapter 3. New Packages

3.1. RHBA-2012:0286 — new package: binutils220

A new binutils220 package is now available for Red Hat Enterprise Linux 5.

[Updated 26 April 2012]

This advisory has been updated with the correct package introduction (the first paragraph) in the Problem Description section. The package included in this revised update has not been changed in any way from the package included in the original advisory.

The binutils220 package provides an assembler and disassembler which understand the specific instructions for the AMD FX processor microarchitecture (Bulldozer) used by the gcc44 compiler. The gcc44 compiler on Red Hat Enterprise Linux 5 can issue Bulldozer specific instructions that can not be handled by the system assembler.

This enhancement update adds the binutils220 package to Red Hat Enterprise Linux 5. (BZ#669190)

All users who require the gcc44 compiler are advised to install this new package.

3.2. RHEA-2012:0224 — new package: iotop

A new iotop package is now available for Red Hat Enterprise Linux 5.

The iotop package provides a program with a UI similar to the top utility. The program watches I/O usage information output by the Linux kernel and displays a table of current I/O usage by processes on the system.

This enhancement update adds the iotop package to Red Hat Enterprise Linux 5. (BZ#545526)

All users who require iotop are advised to install this new package.

3.3. RHEA-2012:0220 — new package: mysql-connector-odbc64

A new mysql-connector-odbc64 package is now available for Red Hat Enterprise Linux 5.

The mysql-connector-odbc64 package provides an ODBC driver for the MySQL database, for use with unixODBC64.

This enhancement update adds the new mysql-connector-odbc64 package to Red Hat Enterprise Linux 5. (BZ#742599)

Users who are not encountering ODBC compatibility issues do not need to install this package. Users who need to interoperate with third-party ODBC drivers are advised to install unixODBC64, and then install mysql-connector-odbc64 if they need to use unixODBC64 with a MySQL database server.

3.4. RHEA-2012:0171 — new package: pixman

A new pixman package is now available for Red Hat Enterprise Linux 5.

The pixman package provides a low-level pixel manipulation library and offers features like image compositing and trapezoid rasterization.

This enhancement update adds the pixman package to Red Hat Enterprise Linux 5. (BZ#718810)

Note

The pixman package is a dependency of spice-client.

All users who require pixman are advised to install this new package.

3.5. RHEA-2012:0221 — new package: postgresql-odbc64

A new postgresql-odbc64 package is now available for Red Hat Enterprise Linux 5.

The postgresql-odbc64 package contains an ODBC driver for the PostgreSQL database, for use with the unixODBC64 package.

This enhancement update adds the new postgresql-odbc64 package to Red Hat Enterprise Linux 5. (BZ#742602)

Users who are not encountering ODBC compatibility issues do not need to install this package. Users who need to interoperate with third-party ODBC drivers are advised to install unixODBC64, and then install postgresql-odbc64 if they need to use unixODBC64 with a PostgreSQL database server.

3.6. RHEA-2012:0183 — new package: python-ctypes

A new python-ctypes package is now available for Red Hat Enterprise Linux 5.

The python-ctypes package provides a foreign function library for Python. It provides C compatible data types, and allows calling functions in DLLs or shared libraries. It can be used to wrap these libraries in pure Python.

This enhancement update adds the python-ctypes package to Red Hat Enterprise Linux 5. (BZ#601661)

Note

This package is being added as a dependency of the iotop package.

All users who require python-ctypes are advised to install this new package.

3.7. RHEA-2012:0172 — new package: spice-client

A new spice-client package is now available for Red Hat Enterprise Linux 5.

SPICE is a remote display system built for virtual environments, this package provides the client.

This enhancement update adds the spice-client package to Red Hat Enterprise Linux 5. (BZ#718817)

All users who require spice-client are advised to install this new package.

3.8. RHEA-2012:0170 — new package: spice-protocol

A new spice-protocol package is now available for Red Hat Enterprise Linux 5.

The spice-protocol package provides header files describing the SPICE protocol and the para-virtual graphics card QXL. This package is required to build spice-clients.

This enhancement update adds spice-protocol to Red Hat Enterprise Linux 5. (BZ#718811)

All SPICE users are advised to install this new package.

3.9. RHEA-2012:0290 — new package: subscription-manager-migration-data

A new subscription-manager-migration-data package is now available for Red Hat Enterprise Linux 5.

The new Subscription Management tooling allows users to understand the specific products which have been installed on their machines, and the specific subscriptions which their machines consume.

This enhancement update adds the subscription-manager-migration-data package to Red Hat Enterprise Linux 5. The package allows for migrations from Red Hat Network Classic Hosted to hosted certificate-based subscription management. (BZ#754492)

All users who require subscription-manager-migration-data are advised to install this new package.

3.10. RHEA-2012:0225 — new package: virt-who

A new virt-who package is now available for Red Hat Enterprise Linux 5.

The virt-who package provides an agent that collects information about virtual guests present in the system and reports them to the subscription manager.

This enhancement update adds the new virt-who package to Red Hat Enterprise Linux 5. (BZ#725839)

All users who require virt-who are advised to install this new package.

3.11. RHEA-2012:0222 — new packages: unixODBC64

New unixODBC64 packages are now available for Red Hat Enterprise Linux 5.

The unixODBC64 packages contain a library for use by programs that use the ODBC standard to connect to database servers. The unixODBC64 package provides a newer version of the ODBC manager library than is provided in the existing Red Hat Enterprise Linux 5.5 unixODBC package.

This enhancement update adds the new unixODBC64 package to Red Hat Enterprise Linux 5. (BZ#742597)

Users who are not encountering ODBC compatibility issues do not need to install these packages. Users who need to interoperate with third-party ODBC drivers are advised to install unixODBC64-libs and possibly unixODBC64, and then install postgresql-odbc64 and/or mysql-connector-odbc64 if needed.

Chapter 4. Package Updates

4.1. acl

4.1.1. RHBA-2012:0242 — acl bug fix update

Updated acl packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

Access Control Lists (ACLs) are used to define fine-grained discretionary access rights for files and directories. The acl packages contain the getfacl and setfacl utilities needed for manipulating access control lists.

Bug Fixes

BZ#536766

Prior to this update, the "-h" and "-v" options of the getfacl and setfacl utilities were not working although they were listed in the documentation. With this update, a patch has been applied and these options are now recognized by the getfacl and setfacl utilities as expected.

BZ#580572

Prior to this update, the getfacl and setfacl utilities failed to preserve the SUID and SGID Sticky Bits along with ACLs. Consequently, after restoring ACLs from a file using the "setfacl --restore" command, all the SUID and SGID Sticky Bits were missing. This update applies backported patches from the upstream package and the problem no longer occurs in the scenario described.

All users of acl are advised to upgrade to these updated packages, which fix these bugs.

4.2. acpid

4.2.1. RHBA-2011:1786 — acpid bug fix update

An updated acpid package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The acpid package contains a daemon that dispatches Advanced Configuration and Power Interface (ACPI) events to user-space programs.

Bug Fixes

BZ#729769

Prior to this update, the acpid daemon repeatedly wrote a number of CPU events to the /var/log/acpid file on certain hardware that was set up for high performance. With this update, the acpid daemon has been optimized so that the CPU events are no longer logged to /var/log/acpid.

BZ#545760

The acpid package contains a trigger scriptlet that returns a non-zero exit code if the /var/log/acpid log file does not exist. Prior to this update, if the acpid daemon was installed but never started on the system and the /var/log/acpid file did not exist, the scriptlet did not function properly and caused the package update process to fail, which could have resulted in two

different acpid packages being installed on the system and registered with the RPM database (rpmdb). With this update, the acpid package has removed the spurious acpid record from rpmdb so that the problem is now fixed.

All users of acpid are advised to upgrade to this updated package, which fixes these bugs.

4.3. alsa-utils

4.3.1. RHEA-2012:0182 — alsa-utils enhancement update

An updated alsa-utils package that adds one enhancement is now available for Red Hat Enterprise Linux 5.

The alsa-utils package contains command line utilities for the Advanced Linux Sound Architecture (ALSA).

Enhancement

BZ#650110

The alsa-delay and alsaloop utilities have been added to alsa-utils to manage the system audio delay.

Users of alsa-utils are advised to upgrade to this updated package, which adds this enhancement.

4.4. anaconda

4.4.1. RHBA-2012:0197 — anaconda bug fix and enhancement update

Updated anaconda packages that fix multiple bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

The anaconda package contains portions of the Anaconda installation program that can be run by the user for reconfiguration and advanced installation options.

Bug Fixes

BZ#477748

When performing the kickstart upgrade with a key for advanced platforms, additional repositories were not enabled, and only the base repository packages were upgraded.

BZ#506361

Adding a VT repository to the kickstart file and using the "key --skip" command resulted in an error when trying to install the Virtualization-en-US package.

BZ#566668

Reusing the LVM logical volumes from the previous installation process caused the bootloader program to use the old disk labels so that the system was unable to boot.

BZ#571513

If the file system label ended with the "0" character, this character was stripped so that the existing file system label was different from what was explicitly specified by the user.

BZ#681219

The "CMSCONFFILE" parameter could have contained wrong syntax. This could have resulted in certain Bash errors on IBM S/390.

BZ#689470

Specifying the "CMSDASD" parameter with a hex number using uppercase letters resulted in the kickstart file not being found.

BZ#684220

The installer environment lacked the symbolic links for stdin, stdout, and stderr. As a result, the console output to the files instead of the screen.

BZ#695299

The installer used the maximum LV size limit based on the LVM 1 limits. Now, the maximum LV size limit is based on the LVM 2 limits.

BZ#702024

Only stderr was logged to the output file during the kickstart installation. Now, stdout is also logged.

BZ#703081

Using the parameter "--no-ssh" in kickstart failed to propagate the same parameter to /root/anaconda-ks.cfg.

BZ#703082

The "--no-ssh" parameter was not documented in /usr/share/doc/anaconda-*/kickstart-docs.txt.

BZ#707143

Downloading the Red Hat Enterprise Linux Release Notes resulted in errors, even though the Release Notes were downloaded successfully.

BZ#708121

The /var/log/ directory required by the Subscription Manager logging was not created.

BZ#709880

The list-harddrives script did not work as expected.

BZ#712443

Errors emitted by the kickstart scripts were not properly reported to the user.

BZ#713120

Even though the installation was run with IPv6 enabled, IPv6 was disabled in the installed environment.

BZ#714243

The Solarflare network adapters were not available to the user during the installation.

BZ#718123

The installation performed on an XTS-encrypted partition failed.

BZ#719578

When specifying the network mask during the manual network setup using the dotted format, a spurious error message was displayed.

BZ#727774

When using the bnx2i iSCSI adapters, the installer did not read IP from iBFT properly.

BZ#737161

The "dhcptimeout" option was not propagated.

BZ#738186

The "--only-use" ignoredisk parameter did not work so that Anaconda terminated unexpectedly.

BZ#742889

portmap was not available in rescue mode so that the rescue environment was unable to mount NFS volumes.

BZ#756707

Adding "-@conflicts" to the kickstart file did not prevent the conflicting packages from the @conflicts group to be installed if other packages depended on the conflicting packages. Now, the conflicting packages and packages that depend on the conflicting packages are not installed.

BZ#758106, BZ#768082

Pressing Esc in certain Anaconda windows had the same result as clicking "OK". With this update, pressing Esc has the same result as clicking "Cancel".

BZ#709931

The Network Configuration interface localization was incomplete.

BZ#711363

The Installation Number screen did not display links under the pa_IN locale.

Enhancement

BZ#660684

Support for the installation over the IP over InfiniBand (IPoIB) interfaces has been added.

All users are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.5. aspell

4.5.1. RHBA-2011:1372 — aspell bug fix update

An updated aspell package that fixes one bug is now available for Red Hat Enterprise Linux 5.

Aspell is a spelling checker that features compile-time and run-time support for English as well as non-English languages and can spell check TeX, LaTeX, and HTML files.

Bug Fix

BZ#432347

Prior to this update, Aspell terminated unexpectedly with a segmentation fault if an empty file was checked for spelling. This bug was corrected in this update so that Aspell now works as expected.

All users of Aspell are advised to upgrade to this updated package, which fixes this bug.

4.6. aspell-sr

4.6.1. RHBA-2011:1368 — aspell-sr bug fix update

An updated aspell-sr package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The aspell-sr package provides the word list and dictionaries for the Serbian language.

Bug Fix

BZ#681716

Prior to this update, the file name of the spec file in the aspell-sr source package (aspell-sl.spec) was incorrect. With this update, the spec file name has been corrected to aspell-sr.spec.

All users of aspell-sr are advised to upgrade to this updated package, which fixes this bug.

4.7. audit

4.7.1. RHBA-2012:0265 — audit bug fix and enhancement update

Updated audit packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The audit packages contain the user space utilities for storing and searching the audit records

generated by the audit subsystem in the Linux 2.6 kernel.

Upgrade to an upstream version

The audit packages have been upgraded to upstream version 1.8, which provides a number of bug fixes and enhancements over the previous version. (BZ#697013)

Bug Fixes

BZ#654883

When the auditd daemon was in immutable mode and was restarted, the following message appeared: "The audit system is in immutable mode, no rules loaded". This message was not clear and was misleading. The message has been therefore improved to "The audit system is in immutable mode, no changes allowed".

BZ#671261

The audit.rules(7) and auditctl(8) manual pages were not consistent in the order of the "action" and "list" fields for the "-a" option. The auditctl(8) manual page has been modified to inform users that the fields can be used in either order.

BZ#702279

Previously, the autrace utility was not aware of system calls being not available on certain architectures. As a consequence, running the "autrace -r" command on the IBM System z, 64-bit PowerPC, and 32-bit Intel architectures failed to insert audit rules. With this update, autrace is aware of system calls not being available on the aforementioned architectures, and audit rules are now successfully inserted.

BZ#706156

System processes, this means processes with an audit id (auid) of -1, are logged by the audit subsystem. However, if the ausearch utility was used to locate events where the auid was -1, all events were displayed. With this update, the ausearch utility now correctly returns only events with an auid of -1.

Enhancement

BZ#667536

This update adds a new option to the configuration of the audisp syslog plug-in, which allows the plug-in to send syslog audit events to local syslog facilities.

All users of audit are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.8. autofs

4.8.1. RHBA-2011:1435 — autofs bug fix update

An updated autofs package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The autofs utility controls the operation of the automount daemon. The automount daemon automatically mounts file systems when you use them, and unmounts them when they are not busy.

Bug Fix

BZ#750463

The recently released erratum RHBA-2011:1374, that corrected a problem with included map entry removal, introduced a new problem with included map key lookup. The condition that was used with the previous patch was too broad and the map key lookup mechanism failed to find keys in an included multi-mount map entry. The condition has been modified so that keys in multi-mount map entries are now found correctly.

All users of autofs are advised to upgrade to this updated package, which fixes this bug.

4.8.2. RHBA-2011:1374 — autofs bug fix update

An updated autofs package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The autofs utility controls the operation of the automount daemon. The automount daemon automatically mounts file systems when you use them, and unmounts them when they are not busy.

Bug Fix

BZ#744698

Previously, when a mounted autofs entry was removed from the autofs direct map and the map was reloaded before the map entry expired, the mount failed to unmount. If such a file system was unmounted manually, the next time a process tried to access this file system, the process became unresponsive. With this update, conditions preventing this behavior have been included into the code. The file system can now be accessed normally and the process no longer hangs.

All users of autofs are advised to upgrade to this updated package, which fixes this bug.

4.8.3. RHBA-2011:1318 — autofs bug fix update

An updated autofs package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The autofs utility controls the operation of the automount daemon. The automount daemon automatically mounts file systems when you use them, and unmounts them when they are not busy.

Bug Fix

BZ#735935

Prior to this update, automount always used the host's IP address instead of the host names. As a result, users had to look up the host name manually when encountering mount problems. This update modifies the name list check so that automount uses now the host name for hosts that have only one IP address.

All autofs users are advised to upgrade to this updated package, which fixes this bug.

4.8.4. RHBA-2012:0264 — autofs bug fix and enhancement update

An updated autofs package that fixes several bugs and adds one enhancement is now available for Red Hat Enterprise Linux 5.

The autofs utility controls the operation of the automount daemon. The automount daemon automatically mounts and unmounts file systems.

Bug Fixes

BZ#655685

Previously, autofs submounts incorrectly handled shutdown synchronization and lock restrictions. As a consequence, automount could be unresponsive when submounts expired. With this update, the submount shuts down only after the states ST_SHUTDOWN, ST_SHUTDOWN_PENDING, and ST_SHUTDOWN_FORCE, or when the state changes to ST_READY.

BZ#692814

Previously, automount did not correctly parse unmatched brackets in map entry server names. As a consequence, the sanity check for host names in these map entries could fail. Now, unmatched brackets in server names result in a syntax error being reported and the check no longer fails.

BZ#700142

Previously, the automount logged confusing error messages when syntax errors occurred in map entry locations. This update modifies these messages and displays more informative messages were possible.

BZ#700896

Previously, LDAP servers did not correctly return an opaque cookie to check for additional results when getting paged results from the server on 64-bit PowerPC and IBM System z platforms due to slightly different criteria for deciding if there are more results. As a consequence, the autofs internal functions did not detect when paged result sets were not supported. This update modifies the underlying source code so that autofs now correctly detects whether the paged results are updated.

BZ#725536

Previously, an incorrect check for the presence of additional addresses for a host led to the IP address being used for mounting instead of the host name. As a consequence the IP address was displayed instead of the host name when listing system mounts, even when the host had only a single address. This update modifies the check so that the IP address is used only if a host has multiple IP addresses.

BZ#731514, BZ#732333

Previously, incorrect identification of the map entry source caused a failure during the key lookup. As a consequence, map lookups for an automount, where a a key was present in a file map and the same key was also found in an included map, failed if the file map entry was removed and a lookup was performed before a re-load is issued. This update modifies the key lookup code and the lookup works now as expected.

BZ#732332

Previously, automount could become unresponsive when reloading a master map that included a combination of direct and indirect maps due to incorrect lock ordering. This update corrects the logic used to determine if the lookup needs to continue into included maps.

BZ#734675

Previously, map entries were always mounted using proximity and response time instead of bind mounting when adding a random selection of a host if the mount was local. This update modifies this behavior and also adds the "nobind" option to allow the previous behavior to be forced if needed.

BZ#747020

Previously, the map key lookup mechanism did not find keys in an included multi-mount map entry. This update modifies the lookup mechanism so that keys in multi-mount map entries are now found correctly.

BZ#759221

Previously, the stack allocation function of the temporary work space was used within a loop in the function lookup_ghost(). As a consequence, a stack overflow could occur and automount then failed with a segmentation fault. This update corrects the allocation usage and the stack overflows no longer occurs.

Enhancement

BZ#732334

With this update,the "--dumpmaps" option to dump maps has been added to dump in autofs.

All users of autofs are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.9. bind

4.9.1. RHSA-2011:1458 — Important: bind security update

Updated bind packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly.

Security Fix

CVE-2011-4313

A flaw was discovered in the way BIND handled certain DNS queries, which caused it to cache an invalid record. A remote attacker could use this flaw to send repeated queries for this invalid record, causing the resolvers to exit unexpectedly due to a failed assertion.

Users of bind are advised to upgrade to these updated packages, which resolve this issue. After installing the update, the BIND daemon (named) will be restarted automatically.

4.9.2. RHBA-2012:0254 — bind bug fix and enhancement update

Updated bind packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 5.

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named), a resolver library (routines for applications to use when interfacing with DNS), and tools for verifying that the DNS server is operating correctly.

Bug Fixes

BZ#663112

Previously, the "named" name service daemon failed to set the max open files limit to "unlimited" by default. Consequently, the error message "max open files (1024) is smaller than max sockets (4096)" was logged. With this update the problem has been fixed, named now sets max open files limit to "unlimited" as documented, and the problem no longer occurs.

BZ#676242

Prior to this update, the code in libdns which sends DNS requests was not robust enough and suffered from a race condition. If a race condition occurred, the "named" name service daemon logged an error message in the format, "zone xxx.xxx.xxx.in-addr.arpa/IN: refresh: failure trying master xxx.xxx.xxx.xxx#53 (source xxx.xxx.xxx.xxx#0): operation canceled", even when zone refresh was successful. This update improves the code to prevent a race condition in libdns and the error no longer occurs in the scenario described.

BZ#692758

A non-writable working directory is a long time feature on all Red Hat systems. Previously, named wrote "the working directory is not writable" as an error to the system log. This update changes the code so that named now writes this information only into the debug log.

BZ#703451

When the "search" option was present in the "/etc/resolv.conf" file but there were no arguments entered for the option, the contents of the following line in the file was interpreted as the missing argument. Consequently, if the following line contained the only "nameserver" option in the file, the system would have no nameservers specified and therefore fail to resolve any hostnames. With this update the code has been improved, the resolv.conf file is parsed correctly, and the problem no longer occurs in the scenario described.

BZ#712791

The "/usr/sbin/bind-chroot-admin" script created symlinks with a double-slash (//) in the paths. This caused logrotate to fail to rotate "/var/log/named.log" correctly. With this update, the bind-chroot-admin utility is fixed and no longer creates symlinks with a double-slash and as a result "/var/log/named.log" is rotated as expected.

BZ#726120

When /etc/resolv.conf contained nameservers with disabled recursion, nslookup failed to resolve certain host names. With this update, nslookup has been patched and now works as expected in the scenario described.

BZ#733698

During a DNS zone transfer, named sometimes terminated unexpectedly with an assertion failure. With this update, a patch has been applied to make the code more robust, and named no longer crashes in the scenario described.

BZ#758873

The named daemon, configured as master server, sometimes failed to transfer an uncompressible zone. The following error message was logged:

transfer of './IN': sending zone data: ran out of space The code which handles zone transfers has been fixed and this error no longer occurs in the scenario described.

Enhancement

BZ#703442

The manpage of the "dig" utility did not document dig's exit status codes. With this update, the "dig" manual page now describes "/usr/bin/dig" exit codes.

Users are advised to upgrade to these updated bind packages, which fix these bugs and add this enhancement.

4.10. bind97

4.10.1. RHSA-2011:1459 — Important: bind97 security update

Updated bind97 packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly.

Security Fix

CVE-2011-4313

A flaw was discovered in the way BIND handled certain DNS queries, which caused it to cache an invalid record. A remote attacker could use this flaw to send repeated queries for this invalid record, causing the resolvers to exit unexpectedly due to a failed assertion.

Users of bind97 are advised to upgrade to these updated packages, which resolve this issue. After installing the update, the BIND daemon (named) will be restarted automatically.

4.11. binutils

4.11.1. RHBA-2012:0271 — binutils bug fix update

An updated binutils package that fixes three bugs is now available for Red Hat Enterprise Linux 5.

Binutils is a collection of binary utilities for the manipulation of object code in various object file formats.

Bug Fixes

BZ#728404

Prior to this update, got2 offset addends could, under certain circumstances, be wrongly incorporated into the trampoline if code at a PLTREL24 relocation with got2 offset addends referenced a symbol that was resolved locally instead of going through the Procedure Linkage Table (PLT). As a result, the trampoline transferred the code to the wrong target. With this update, the addend of the relocation is, where necessary, cleared. Now, the computation of the trampoline's target address is correct.

BZ#748927

Prior to this update, the dl debug state RT_CONSISTENT incorrectly occurred before applying dynamic relocations. As a consequence, debugging tools could not correctly monitor this call. This update adds systemtap-probes at a superset of the locations where the state RT_CONSISTENT was called.

BZ#755872

Prior to this update, the linker did not allow the local-exec Thread-local storage (TLS) model with -fPIC when creating an executable. As a consequence, the local-exec TLS model did not work with executables compiled with position-independent code (PIC) or position-independent executables (PIE) when creating an executable. This update modifies the underlying code to only disallow the local-exec TLS model when creating a shared library.

Users are advised to upgrade to this updated binutils package, which fixes these bugs.

4.12. boost

4.12.1. RHBA-2011:1246 — boost bug fix update

Updated boost packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The boost packages provide free peer-reviewed portable C++ source libraries with emphasis on libraries which work well with the C++ Standard Library.

Bug Fix

BZ#727895

An application compiled against the boost package version prior to 1.33.1-10.el5_7.2, and run with this exact version installed, could be killed by a SIGSEGV signal due to mismatch in the application binary interface (ABI) of the regular expression library. That failure could only be fixed by recompiling the application. This updated package rectifies the ABI changes in aforementioned version of the boost package.

Important: any client application which was recompiled against boost version 1.33.1-10.el5_7.2 should be recompiled against this updated package to ensure a stable ABI and avoid any potential incompatibility.

Users of boost are advised to upgrade to these updated packages, which fix this bug.

4.12.2. RHBA-2011:1149 — boost bug fix update

Updated boost packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The boost package provides free peer-reviewed portable C++ source libraries with emphasis on libraries which work well with the C++ Standard Library.

Bug Fix

BZ#727895

Prior to this update, when several regular expression objects were created simultaneously, such as in a multi-threaded program, the construction of one of them sometimes failed. With this update, the object variables have been moved from the shared memory to the stack, thereby making the constructing function thread safe.

Users of boost are advised to upgrade to these updated packages, which fix this bug.

4.12.3. RHSA-2012:0305 — Low: boost security and bug fix update

Updated boost packages that fix two security issues and two bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The boost packages provide free, peer-reviewed, portable C++ source libraries with emphasis on libraries which work well with the C++ Standard Library.

Security Fixes

CVE-2008-0171

Invalid pointer dereference flaws were found in the way the Boost regular expression library processed certain, invalid expressions. An attacker able to make an application using the Boost library process a specially-crafted regular expression could cause that application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2008-0172

NULL pointer dereference flaws were found in the way the Boost regular expression library processed certain, invalid expressions. An attacker able to make an application using the Boost library process a specially-crafted regular expression could cause that application to crash.

Red Hat would like to thank Will Drewry for reporting these issues.

Bug Fixes

BZ#472384

Prior to this update, the construction of a regular expression object could fail when several regular expression objects were created simultaneously, such as in a multi-threaded program. With this update, the object variables have been moved from the shared memory to the stack.

Now, the constructing function is thread safe.

BZ#567722

Prior to this update, header files in several Boost libraries contained preprocessor directives that the GNU Compiler Collection (GCC) 4.4 could not handle. This update instead uses equivalent constructs that are standard C.

All users of boost are advised to upgrade to these updated packages, which fix these issues.

4.13. bootparamd

4.13.1. RHBA-2011:1190 — bootparamd bug fix update

An updated bootparamd package that fixes one bug is now available for Red Hat Enterprise Linux 5.

Bootparamd is a server utility that provides information needed by diskless clients to boot. It consults the /etc/bootparams file for the required information.

Bug Fix

BZ#729306

Previously, the bootparamd utility did not convert network byte order (big-endian) to host byte order (little-endian on Linux and x86 platforms). Consequently, the sort functionality of a router's IP addresses did not work correctly because the ulong_compare() function compared values in reverse order. This bug has been fixed, and sorting now works properly in the described scenario.

All users of bootparamd are advised to upgrade to this updated package, which fixes this bug.

4.14. busybox

4.14.1. RHBA-2012:0026 — busybox bug fix update

Updated busybox packages that fix one bug are now available for Red Hat Enterprise Linux 5.

BusyBox is a binary that combines a large number of common system utilities into a single executable. BusyBox provides replacements for most GNU fileutils, shellutils, and so on.

Bug Fix

BZ#761532

Previously, the findfs command did not release used file descriptors. Therefore, the system could run out of free file descriptors on the systems with a large amount (thousands) of block devices. As a consequence, findfs failed to check all existing block devices on the system which could cause other problems, such as a kdump service failure. This update modifies BusyBox so that findfs now releases file descriptors properly and checks all block devices as expected.

All users of BusyBox are advised to upgrade to these updated packages, which fix this bug.

4.14.2. RHSA-2012:0308 — Low: busybox security and bug fix update

Updated busybox packages that fix two security issues and two bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

BusyBox provides a single binary that includes versions of a large number of system commands, including a shell. This can be very useful for recovering from certain types of system failures, particularly those involving broken shared libraries.

Security Fixes

CVE-2006-1168

A buffer underflow flaw was found in the way the uncompress utility of BusyBox expanded certain archive files compressed using Lempel-Ziv compression. If a user were tricked into expanding a specially-crafted archive file with uncompress, it could cause BusyBox to crash or, potentially, execute arbitrary code with the privileges of the user running BusyBox.

CVE-2011-2716

The BusyBox DHCP client, udhcpc, did not sufficiently sanitize certain options provided in DHCP server replies, such as the client hostname. A malicious DHCP server could send such an option with a specially-crafted value to a DHCP client. If this option's value was saved on the client system, and then later insecurely evaluated by a process that assumes the option is trusted, it could lead to arbitrary code execution with the privileges of that process. Note: udhcpc is not used on Red Hat Enterprise Linux by default, and no DHCP client script is provided with the busybox packages.

Bug Fixes

BZ#689659

Prior to this update, the cp command wrongly returned the exit code 0 to indicate success if a device ran out of space while attempting to copy files of more than 4 gigabytes. This update modifies BusyBox, so that in such situations, the exit code 1 is returned. Now, the cp command shows correctly whether a process failed.

BZ#756723

Prior to this update, the findfs command failed to check all existing block devices on a system with thousands of block device nodes in "/dev/". This update modifies BusyBox so that findfs checks all block devices even in this case.

All users of busybox are advised to upgrade to these updated packages, which correct these issues.

4.15. cdparanoia

4.15.1. RHBA-2012:0208 — cdparanoia bug fix update

Updated cdparanoia packages that fix a bug are now available for Red Hat Enterprise Linux 5.

The cdparanoia utility is responsible for extracting content from audio CDs.

Bug Fix

BZ#502569

Due to an error in the cdparanoia SGIO (SCSI Generic I/O) layer probing, the gnome-cd utility terminated unexpectedly with a segmentation fault when accessing a device linked to the /dev/cdrom device file but using another device file name. An upstream patch has been provided to address this issue and gnome-cd no longer crashes in the described scenario.

Users of cdparanoia are advised to upgrade to these updated packages, which fix this bug.

4.16. certmonger

4.16.1. RHBA-2011:1842 — certmonger bug fix update

An updated certmonger package that fixes one bug is now available for Red Hat Enterprise Linux 5.

[Updated 20 December 2011] This advisory has been updated with the correct product name (that is, Red Hat Enterprise Linux 5) in the Details section. The package included in this revised update has not been changed in any way from the package included in the original advisory.

The certmonger service monitors certificates, warning of their impending expiration, and optionally attempting to re-enroll with supported CAs (Certificate Authorities).

Bug Fix

BZ#767573

The RHSA-2011-1533 security advisory, which fixed a security vulnerability in the IPA (Identity, Policy and Audit) web-based service, caused incompatibility with older versions of certmonger. As a consequence, certmonger was unable to correctly submit enrollment requests to IPA's CA. With this update, certmonger has been modified and it now operates correctly with newer versions of IPA. Interoperability with older versions of IPA remains unaffected.

All users of certmonger are advised to upgrade to this updated package, which fixes this bug.

4.16.2. RHBA-2011:1238 — certmonger bug fix update

An updated certmonger package is now available for Red Hat Enterprise Linux 6.

The certmonger service monitors certificates, warning of their impending expiration, and optionally attempting to re-enroll with supported CAs (Certificate Authorities).

Bug Fix

BZ#729803

When submitting a signing request to a Red Hat IPA (Identity, Policy, Audit) CA, certmonger is expected to authenticate using the client's host credentials, and to delegate the client's credentials to the server. Recent updates to libraries on which certmonger depends changed delegation of client credentials from a mandatory operation to an optional operation that is no longer enabled by default, which effectively broke certmonger's support for IPA CAs.

This update gives certmonger the ability to explicitly request credential delegation when used

with newer versions of these libraries, which introduce an API that allows certmonger to explicitly request that credential delegation be performed.

All certmonger users should upgrade to this updated package, which fixes this bug.

4.16.3. RHBA-2012:0245 — certmonger bug fix and enhancement update

An updated certmonger package that fixes multiple bugs and adds one enhancement is now available for Red Hat Enterprise Linux 5.

The certmonger service monitors certificates as the date at which they become invalid approaches, optionally attempting to re-enroll with a supported certificate authority (CA) to keep the services which use the certificates running without incident.

The certmonger service, which was initially introduced as a Technology Preview, is now fully-supported. (BZ#665317)

Bug Fixes

BZ#712072

Prior to this update, ipa-getcert list calls from non-root users logged the misleading message ""Number of certificates and requests being tracked: 0". This update modifies the underlying code to display the correct message "Insufficient access. Please retry operation as root." when non-root users call ipa-getcert list.

BZ#756745

Prior to this update, starting the certmonger service as non-root user looged the uninformative message "Error connecting to D-Bus.". This update modifies the underlying code to display the correct message "Insufficient access. Please retry operation as root." when non-root users start the certmonger service.

BZ#757883

Prior to this update, the IPA web-based service was not compatibile with certmonger. As a consequence, certmonger was unable to correctly submit enrollment requests to IPA's CA. With this update, certmonger has been modified and it now operates correctly with newer versions of IPA.

Enhancement

BZ#727864

Prior to this update, libcurl could not delegate Kerberos tickets via XML-RPC to authenticate with Identity, Policy and Audit (IPA). This update adds support for the xmlrpc-c API to allow for Generic Security Services Application Program Interface (GSSAPI) delegation.

All users of the certmonger service are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.17. Cluster_Administration

4.17.1. RHBA-2012:0175 — Cluster_Administration bug fix and enhancement update

Updated Cluster_Administration packages that fix numerous bugs and add several enhancements are now available for Red Hat Enterprise Linux 5.

The Cluster Administration book describes the configuration and management of Red Hat cluster systems for Red Hat Enterprise Linux 5.

The Cluster Administration book has been updated to version 5.8, which provides a number of bug fixes and enhancements over the previous version. (BZ#727332)

All users of the Cluster Administration book are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.18. clustermon

4.18.1. RHBA-2012:0292 — clustermon bug-fix update

Updated clustermon packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The clustermon packages are used for remote cluster management. The modclusterd service provides an abstraction of cluster status used by conga and by the Simple Network Management (SNMP) and Common Information Model (CIM) modules of clustermon.

Bug Fixes

BZ#618321

Prior to this update, under certain circumstances, outgoing queues in inter-node communication of the modclusterd service could grow over time. To prevent this behavior, the inter-node communication is now better balanced and queues are restricted in size. Forced queue interventions are logged in the /var/log/clumond.log file.

BZ#736814

Prior to this update, execution of external programs (such as /usr/sbin/clustat) from within the modclusterd daemon or ricci's helper program, modcluster, could make these unresponsive. In such a case, processes depending on the programs could also become unresponsive or indicate an error. For example, in tools like luci, the affected node could be listed as having communications problems, or the cluster creation could become unresponsive. Patches have been applied to address this issue, and deadlocks no longer occur when executing external programs.

All users of clustermon are advised to upgrade to these updated packages, which fix these bugs.

4.19. cman

4.19.1. RHBA-2012:0053 — cman bug fix update

An updated cman package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The Cluster Manager (cman) utility provides user-level services for managing a Linux cluster.

Bug Fix

BZ#782833

Due to the latest changes of the Representational State Transfer (REST) API for Red Hat Enterprise Virtualization 3, the fence_rhevm fencing agent failed to show correct status of virtual machines. Also, the URL of the API entry point was changed in the REST API, which caused the fence_rhevm to be unable to send GET requests to the REST API. With this update, fence_rhevm has been updated to match the current REST API.

All users of cman are advised to upgrade to this updated package, which fixes this bug.

4.19.2. RHBA-2011:1337 — cman bug fix update

An updated cman package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The Cluster Manager (cman) utility provides user-level services for managing a Linux cluster.

Bug Fix

BZ#740181

Prior to this update, only one fenced option could be specified when using the cman init script. This update modifies FENCED_OPTS so that more than one option can be specified.

All cman users are advised to upgrade to this updated package, which fixes this bug.

4.19.3. RHEA-2011:1217 — cman enhancement update

An enhanced cman package is now available for Red Hat Enterprise Linux 5.

The Cluster Manager (CMAN) utility provides user-level services for managing a Linux cluster.

Enhancement

BZ#731306

With this update, the cman init script now allows a user to pass specific options to the fence daemon, fenced.

Users of cman are advised to upgrade to this updated package, which adds this enhancement.

4.19.4. RHBA-2012:0167 — cman bug fix and enhancement update

An updated *cman* package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 5.

The Cluster Manager (cman) utility provides user-level services for managing a Linux cluster.

Bug Fixes

BZ#739966

The **FENCED_OPTS** variable was escaped incorrectly. Consequently, only the first option passed to **FENCED_OPTS** was processed correctly and any further options were ignored. This update corrects the escaping of the **FENCED_OPTS** and all options are now honored as expected.

BZ#590101

The **shutdown_con** variable was not cleared if the shutdown process was killed. This caused the **cman** service to terminate with a segmentation fault in the **unbind_con()** function if another process shut down the utility. The **shutdown_con** variable is now cleared after the shutdown process is canceled and the utility shuts down gracefully.

BZ#727215

The **cman** utility released the connection prematurely on shut down. As a consequence, **cman** sent spurious messages to the **syslog** utility. With this update, the connection is released after the shutdown process has finished and the spurious messages are no longer sent to **syslog**.

BZ#730634

The **fence_drac5** agent did not grant enough time to the Dell Remote Access controller 5 (DRAC5) hardware to update its internal connection count. This update adds a sleep function to the respective code to provide the firmware enough time to clean old sessions and new connections are now established as expected. If you are using the DRAC5 firmware released earlier than version 1.60, the firmware needs to be upgrade to 1.60 or later to fix this bug.

BZ#746599

The cman **service_cman.lcrso** service did not provide debug symbols because the service was built without the **-g** CFLAGS option. The **gcc** compiler then built the debuginfo files without debugging symbols. This flag has been added to the Makefile and the service is now built with debugging symbols as expected.

BZ#745536

The **ping** command examples on the qdisk(5) manual page were missing the **-w** option. If the **ping** command is run without the option, the action can timeout. With this update, the **-w** option has been added to the example **ping** commands.

BZ#689851

On a blade removal, the prompt does not signal that the blade is no longer available. Previously, the fence **reboot** command with the **--missing-as-off** option relied on the prompt, and the fencing failed. With this update, fence reboot works as expected.

BZ#732773

The **fence_ipmilan** agent did not parse the arguments of the **passwd_script** option in the **cluster.conf** file and fencing could fail. The arguments are now parsed correctly and fencing succeeds as expected.

BZ#704243

The **qdiskd** daemon failed to update a Quorum disk device after it was changed and the **clustat** command showed an old qdisk device as being used. The interactions between the **cman** utility and **qdisk** utility have been improved including cman logging, error reports, and checks of Quorum API usage. The **qdiskd** daemon can now update device names in cman; the error checking at qdickd startup has been improved.

BZ#718194

Due to a mistake in the **fence_drac5** list operation, Dell Drac CMC devices were not working correctly as fence devices. The **fence_drac5** list operation has been fixed for Dell DRAC CMC devices.

BZ#727492

The cman(5) manual page contained an invalid multicast address in the example of a multicast address overriding. The example has been changed and now contains a valid multicast address.

BZ#715107

Previously, the **fence_vmware_soap** utility did not expose valid virtual machine names for fencing. The **fence_vmware_soap()** function has been updated to support unique virtual machine names.

BZ#753797

Fencing a Red Hat Enterprise Linux cluster node running in a virtual machine on VMWare with the fence_soap_vmware fence agent failed with the following error message:

```
KeyError: 'config.uuid'
```

This happened because the fencing agent was not able to work with more than one hundred machines in the cluster. With this update, the underlying code has been modified to support fencing of such clusters.

Enhancements

BZ#731167

The **fence_rhevm** utility has been updated to conform to the changes in the RHEV-M 3.0 API: The RUNNING status has been changed to the UP status.

BZ#730639

The user can now pass specific options to the **fenced** daemon.

BZ#726731

The fence_ipmilan fencing agent now supports the **-L** option for logging in as a non-privileged user and fence with the user session privileges.

BZ#749245

The fence_scsi fencing mechanism now works with CLVM (Clustered Logical Volume Manager) when High Availability LVM (HA-LVM) in CLVM mode is used to provide a data store for services.

All *cman* users are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.20. cmirror

4.20.1. RHBA-2012:0256 — cmirror bug fix update

An updated cmirror package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The cmirror package provides user-level tools for managing cluster mirroring. Cmirror is needed for LVM-based mirroring (RAID1) in a cluster environment.

Bug Fixes

BZ#566799

Prior to this update, cmirror could become suspended with the pvmove command on a segmented volume when attempting to connect to the checkpoint service. With this update, cmirror uses a finite number of retries when connecting to the checkpoint service and no longer becomes suspended.

BZ#713295

Prior to this update, the cmirror init script was by default switched on after the RPM installation, while all the other cluster init scripts were switched off. With this update, the cmirror init script is by default switched off.

All users of cmirror are advised to upgrade to this updated package, which fixes these bugs.

4.21. comps-extras

4.21.1. RHBA-2012:0294 — comps-extras bug fix update

An updated comps-extras package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The comps-extras package contains images for the components included in Fedora.

Bug Fix

BZ#761522

Previously, user interface of the Anaconda installer was missing variant icons for Cluster, Cluster Storage and Virtualization. With this update, these icons have been added.

Users of comps-extras are advised to upgrade to this updated package, which fixes this bug.

4.22. conga

4.22.1. RHBA-2011:1421 — conga bug fix update

Updated conga packages that fix a bug are now available for Red Hat Enterprise Linux 5.

Conga is an agent/server architecture for remote administration of systems. It provides a convenient method for creating and managing clusters built with Red Hat Cluster Suite. It also offers an interface for managing sophisticated storage configurations like those often built to support clusters. The agent component is called "ricci", and the server is called "luci".

Bug Fix

BZ#741169

Prior to this update, when a new cluster was being created with luci, and luci tried to list, install or update cluster packages, the installation process could become unresponsive and could not finish. With this update, the bug has been fixed, and the creation of a new cluster now completes successfully in the described scenario.

Users of conga are advised to upgrade to these updated packages, which fix this bug.

4.22.2. RHSA-2012:0151 — Moderate: conga security, bug fix and enhancement update

Updated conga packages that fix multiple security issues, multiple bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The Conga project is a management system for remote workstations. It consists of luci, which is a secure web-based front end, and ricci, which is a secure daemon that dispatches incoming messages to underlying management modules.

Security Fixes

CVE-2010-1104, **CVE-2011-1948**

Multiple cross-site scripting (XSS) flaws were found in luci, the conga web-based administration application. If a remote attacker could trick a user, who was logged into the luci interface, into visiting a specially-crafted URL, it would lead to arbitrary web script execution in the context of the user's luci session.

Bug Fixes

BZ#709478

Previously, due to incorrect permissions from **libvirt**, the **`ricci`** daemon failed to detect if a host was capable of running a virtual machine. As a consequence, the **`Add a Virtual Machine Service`** tab was not displayed under **`Services`** when using the **luci** tool. With this update, calling the **virsh** program is now avoided, and the **`Add a Virtual Machine Service`** tab is now displayed under **`Services`**.

BZ#723000

If the user modified in **luci** the **name** attribute of a shared resource that was attached to an existing service, the **ref** attribute for the shared resource in the **`cluster.conf`** file was not updated. With this update, luci is modified so that the **ref** attribute in **`cluster.conf`** is correctly updated to reflect the new name of the resource.

BZ#723188

Previously, **luci** did not allow users to modify the **`__max_restarts`** and

__restart_expire_time attributes for independent subtrees, but only for non-critical resources. If the user tried to set values for "Maximum number of restart failures before giving up (applies only for non-critical resources)" and "Restart expire time (applies only for non-critical resources)", these values were not added for the resource in the **cluster.conf** file. This update modifies luci so that users are now able to modify the aforementioned values in luci.

BZ#732483

Prior to this update, execution of external programs (such as **/usr/sbin/clustat**) from within the **modclusterd** daemon or ricci's helper program, **modcluster**, could make these unresponsive. In such a case, processes depending on them could also become unresponsive or indicate an error. For example, in tools like **luci**, the affected node could be listed as having communications problems, or the cluster creation could become unresponsive. Patches have been applied to address this issue, and deadlocks no longer occur when executing external programs.

BZ#734562

When adding a resource to a service, **luci** only checked to verify that the name of the resource did not match the name of a resource in the resources stanza. The **luci** tool did not check to see if any resources in other services shared the same name, and therefore allowed users to create two services with the resources of the same name. This led to unique attribute collisions. With this update, luci's name validation is improved, and adding a resource to a service no longer leads to collisions. In addition, certain error messages have been modified to display more verbose information.

BZ#739600

Previously, users were able to insert the quote character (") with NFS resources in the "resources" section of the cluster configuration in **conga**. The resource data submitted for this service was not properly formed and converted into the **cluster.conf** file. With this update, if the user inserts the quote character, the following error message appears:

```
The resource data submitted for this service is not properly formed
```

BZ#755941

Previously, the **luci_admin restore** command did not fully restore a database to the original state. This was because the **luci_admin** script only added items contained in the previously generated backup XML file. This update adds new options, **-u** (**--update**) and **-r** (**--replace**), that are used to either keep or remove existing configuration when restoring a database.

Enhancement

BZ#751359

The **fence_ipmilan** agent has been updated to support the "-L" option of the **ipmilan** daemon, thus supporting fencing with user session privileges level.

Users of *conga* are advised to upgrade to these updated packages, which correct these issues. After

installing the updated packages, luci must be restarted (**`service luci restart`**) for the update to take effect.

4.23. crash

4.23.1. RHBA-2012:0203 — crash bug fix and enhancement update

An updated crash package that fixes various bugs is now available for Red Hat Enterprise Linux 5

The crash package provides a self-contained tool that can be used to investigate live systems, and kernel core dumps created from the netdump, diskdump, kdump, and Xen/KVM "virsh dump" facilities from Red Hat Enterprise Linux.

Bug Fixes

BZ#715072

The crash package has been upgraded to upstream version 5.1.8, which provides a number of enhancements and bug fixes over the previous version.

BZ#676408

On AMD64 and Intel 64 architectures, the "bt" command failed when the shutdown NMI was issued to a 32-bit task that had executed a "sysenter" instruction and the RSP still contained the zero value loaded from the MSR_IA32_SYSENTER_ESP register. Consequently, the backtrace issued the following warning message:

"WARNING: possibly bogus exception frame"

and was unable to make a transition from the NMI exception stack back to the process stack. With this update, the underlying source code has been modified to address this issue, and the aforementioned command no longer fails.

BZ#713050

On AMD64 and Intel 64 architectures, the "bt" command failed with several backtrace errors for non-crashing active tasks:

"bt: cannot resolve stack trace"

This was due to a failure to properly transition from the shutdown NMI stack back to the process stack. This update fixes these errors, and executing the "bt" command on non-crashing active tasks works as expected.

BZ#716327

KVM virtual systems contain an I/O hole in the physical memory region from 0xe0000000 to 0x100000000 (3.5 GB to 4 GB). If a guest is provisioned with more than 3.5 GB of RAM, then the memory above 3.5 GB is "pushed up" to start at 0x100000000 (4 GB). However, the "ram" device headers in the KVM dumpfiles do not reflect that. As a result, numerous error messages were displayed during invocation, and the session would often fail. With this update, the crash utility takes the I/O hole into account despite the fact that the "ram" device headers in KVM dumpfiles do not; consequently, error messages are no longer displayed during invocation.

BZ#715070

The KVM I/O hole size is currently set to either 1 GB or 512 MB, but its setting is hardwired into the Qemu code that was used to create the dumpfile. The dumpfile is a "savevm" file that is designed to be used for guest migration, and since inter-version save/load operations are not supported, the I/O hole information does not have to be encoded into the dumpfile. Prior to this update, the I/O hole for dumpfiles created by older Qemu version was not being set to 1GB, so if the KVM guest was configured with more than 3GB of memory, the crash session would typically display numerous "read error" messages during session initialization. With this update, the crash session does not return any error messages during session initialization.

All users of crash are advised to upgrade to this updated package, which resolves these issues.

4.24. cups

4.24.1. RHSA-2012:0302 — Low: cups security and bug fix update

Updated cups packages that fix one security issue and various bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The Common UNIX Printing System (CUPS) provides a portable printing layer for Linux, UNIX, and similar operating systems.

CVE-2011-2896

A heap-based buffer overflow flaw was found in the Lempel-Ziv-Welch (LZW) decompression algorithm implementation used by the CUPS GIF image format reader. An attacker could create a malicious GIF image file that, when printed, could possibly cause CUPS to crash or, potentially, execute arbitrary code with the privileges of the "lp" user.

Bug Fixes

BZ#625900

Prior to this update, the "Show Completed Jobs," "Show All Jobs," and "Show Active Jobs" buttons returned results globally across all printers and not the results for the specified printer. With this update, jobs from only the selected printer are shown.

BZ#625955

Prior to this update, the code of the serial backend contained a wrong condition. As a consequence, print jobs on the raw print queue could not be canceled. This update modifies the condition in the serial backend code. Now, the user can cancel these print jobs.

BZ#660518

Prior to this update, the textonly filter did not work if used as a pipe, for example when the command line did not specify the filename and the number of copies was always 1. This update modifies the condition in the textonly filter. Now, the data are sent to the printer regardless of the number of copies specified.

BZ#668009

Prior to this update, the file descriptor count increased until it ran out of resources when the cups daemon was running with enabled Security-Enhanced Linux (SELinux) features. With this update, all resources are allocated only once.

BZ#759081

Prior to this update, CUPS incorrectly handled the en_US.ASCII value for the LANG environment variable. As a consequence, the lpadmin, lpstat, and lpinfo binaries failed to write to standard output if using LANG with the value. This update fixes the handling of the en_US.ASCII value and the binaries now write to standard output properly.

All users of cups are advised to upgrade to these updated packages, which contain backported patches to resolve these issues. After installing this update, the cupsd daemon will be restarted automatically.

4.25. curl

4.25.1. RHBA-2011:1188 — curl bug fix update

An updated curl package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The curl package provides the libcurl library and the cURL command line tool for transferring data using various protocols, including FTP, HTTP, Gopher, Telnet, and DICT. Both, libcurl and cURL, support many useful capabilities, such as user authentication, proxy support, FTP uploading, HTTP POST and PUT methods, SSL certificates, and file transfer resume.

Bug Fix

BZ#727884

As a solution to a security issue, GSSAPI credential delegation was disabled, which broke the functionality of the applications that were relying on delegation, which was incorrectly enabled by libcurl. To fix this issue, the CURLOPT_GSSAPI_DELEGATION libcurl option has been introduced in order to enable delegation explicitly when applications need it. All applications using GSSAPI credential delegation can now use this new libcurl option to be able to run properly.

All users of cURL and libcurl are advised to upgrade to this updated package, which resolves this issue. All running applications using libcurl have to be restarted for the update to take an effect.

4.25.2. RHBA-2012:0241 — curl bug fix and enhancement update

An updated curl package that fixes multiple bugs and adds two enhancements is now available for Red Hat Enterprise Linux 5.

The curl package provides the libcurl library and the cURL command line tool for transferring data using various protocols, including FTP, HTTP, Gopher, Telnet, and DICT. Both, libcurl and cURL, support many useful capabilities, such as user authentication, proxy support, FTP uploading, HTTP POST and PUT methods, SSL certificates, and file transfer resume.

Bug Fixes

BZ#652557

In the FTP implementation, libcurl incorrectly called the accept() function from a system library, which caused a stack overflow under certain circumstances. This update applies a backported upstream patch that corrects this bug, and the stack overflow no longer occurs.

BZ#655073

Previously, an attempt to send an LDAP request through an HTTP proxy tunnel ended up with cURL trying to connect to the LDAP server directly using a wrong port number. With this update, the underlying source code has been modified to fix this problem, and cURL now works as expected.

BZ#688871

Previously, the "multi" interface of libcurl was broken, which caused the "git push" command to work incorrectly over the Web Distributed Authoring and Versioning (WebDAV) protocol. This update applies an upstream patch, which corrects counting of active connections in the "multi" interface. The "git push" command now works as expected over WebDAV.

BZ#723643

As a solution to a security issue, GSSAPI credential delegation was disabled, which broke the functionality of the applications that were relying on delegation, which was incorrectly enabled by libcurl. To fix this problem, the CURLOPT_GSSAPI_DELEGATION libcurl option has been introduced in order to enable delegation explicitly when applications need it. All applications using GSSAPI credential delegation can now use this new libcurl option to be able to run properly.

Enhancements

BZ#657396

Previously, curl did not support proxy authentication using Kerberos. With this update, underlying code has been modified and curl now allows Kerberos proxy authentication by using the "--proxy-negotiate" option.

BZ#746849

The cURL utility did not allow Kerberos credential delegation although the libcurl library provided appropriate support for this functionality. This update introduces a new option, "--delegation", which enables Kerberos credential delegation in cURL.

All users of curl are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements. All running applications that use libcurl have to be restarted for this update to take effect.

4.26. cvs

4.26.1. RHBA-2012:0253 — cvs bug fix update

Updated cvs packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

The Concurrent Versions System (CVS) is a version control system that can record the history of your files. CVS only stores the differences between versions, instead of every version of every file you have

ever created. CVS also keeps a log of who, when, and why changes occurred.

Bug Fixes

BZ#538376

Previously, the CVS server did not pass the client address to the Pluggable Authentication Modules (PAM) system. As a result, it was not possible to distinguish clients by the network address with the PAM system and the system was not able to utilize the client address and use it for the authentication or authorization purposes. With this update, the client network address is passed to the PAM subsystem as a remote host item (PAM_RHOST). Also, the terminal item (PAM_TTY) is set to a dummy value "cvs" because some PAM modules cannot work with an unset value.

BZ#769298

Previously, when using the "cvs rtag" command with a repository, which included the "." character in the repository path, the CVS server hit the assertion test and terminated. With this update, the assertion check for "." in the CVSROOT path has been removed as CVS can process this path safely now so that "cvs rtag" works with repositories with "." in the CVSROOT path as expected.

All CVS users are advised to upgrade to these updated packages, which fix these bugs.

4.27. cyrus-imapd

4.27.1. RHSA-2011:1508 — Moderate: cyrus-imapd security update

Updated cyrus-imapd packages that fix two security issues are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The cyrus-imapd packages contain a high-performance mail server with IMAP, POP3, NNTP, and Sieve support.

Security Fixes

CVE-2011-3372

An authentication bypass flaw was found in the cyrus-imapd NNTP server, nntpd. A remote user able to use the nntpd service could use this flaw to read or post newsgroup messages on an NNTP server configured to require user authentication, without providing valid authentication credentials.

CVE-2011-3481

A NULL pointer dereference flaw was found in the cyrus-imapd IMAP server, imapd. A remote attacker could send a specially-crafted mail message to a victim that would possibly prevent them from accessing their mail normally, if they were using an IMAP client that relies on the server threading IMAP feature.

Red Hat would like to thank the Cyrus IMAP project for reporting the CVE-2011-3372 issue. Upstream acknowledges Stefan Cornelius of Secunia Research as the original reporter of CVE-2011-3372.

Users of cyrus-imapd are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing the update, cyrus-imapd will be restarted automatically.

4.27.2. RHSA-2011:1317 — Important: cyrus-imapd security update

Updated cyrus-imapd packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The cyrus-imapd packages contain a high-performance mail server with IMAP, POP3, NNTP, and Sieve support.

Security Fix

CVE-2011-3208

A buffer overflow flaw was found in the cyrus-imapd NNTP server, nntpd. A remote user able to use the nntpd service could use this flaw to crash the nntpd child process or, possibly, execute arbitrary code with the privileges of the cyrus user.

Red Hat would like to thank Greg Banks for reporting this issue.

Users of cyrus-imapd are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the update, cyrus-imapd will be restarted automatically.

4.28. dapl

4.28.1. RHBA-2012:0252 — dapl bug fix update

Updated dapl packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The dapl package provides a user-space implementation of the DAT 2.0 API that allows applications to utilize high-performance network technologies such as InfiniBand and iWARP.

Bug Fixes

BZ#634323

Previously, an error in the code path in the uDAPL layer did not allow the cp_ptr entry to be cleaned up correctly in the internal link list. This could cause new connections to fail. With this update, the entry is cleaned up correctly and subsequent connections work as expected.

BZ#634324

Previously, dapl could leak file descriptors and the application could terminate. With this update, the leak is closed and dapl behaves as expected.

BZ#636193

Previously, verbs CQ and completion channels were not correctly disconnected and freed,

which could cause an application crash. With this update, verbs CQ and completion channels behave as expected.

BZ#636197

Previously, an error in the code path in the compat-dapl layer did not allow the cp_ptr entry to be cleaned up correctly in the internal link list. This could cause new connections to fail. With this update, the entry is cleaned up correctly and subsequent connections work as expected.

BZ#645825

Under certain circumstances, the dat_ia_open() call and the programs using the function could become unresponsive. With this update, the underlying code has been modified and the function behaves as expected.

BZ#658950

Due to an invalid error mapping, when dapl received a signal during the execution of the dapls_evd_dto_wait() function, it could fail to set the correct error type, which may have led to an incorrect operation. With this update, the relevant part of the source code has been modified to return the correct value, and dapl now works as expected.

All dapl users are advised to upgrade to these updated packages, which fix these bugs.

4.29. dbus

4.29.1. RHSA-2011:1132 — Moderate: dbus security update

Updated dbus packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

D-Bus is a system for sending messages between applications. It is used for the system-wide message bus service and as a per-user-login-session messaging facility.

Security Fix

CVE-2011-2200

A denial of service flaw was found in the way the D-Bus library handled endianness conversion when receiving messages. A local user could use this flaw to send a specially-crafted message to dbus-daemon or to a service using the bus, such as Avahi or NetworkManager, possibly causing the daemon to exit or the service to disconnect from the bus.

All users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. For the update to take effect, all running instances of dbus-daemon and all running applications using the libdbus library must be restarted, or the system rebooted.

4.30. Deployment_Guide

4.30.1. RHBA-2012:0178 — Deployment_Guide bug fix and enhancement update

Updated Deployment_Guide packages that fix numerous bugs and add several enhancements are now available for Red Hat Enterprise Linux 5.

The Deployment Guide provides relevant information regarding the deployment, configuration, and administration of Red Hat Enterprise Linux 5.

The Deployment Guide has been updated to version 5.8, which provides a number of bug fixes and enhancements over the previous version. (BZ#720860)

All users of the Deployment Guide are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.31. device-mapper

4.31.1. RHBA-2012:0219 — device-mapper bug fix and enhancement update

Updated device-mapper packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The device-mapper packages provide the dmsetup utility and libdevmapper library required by logical volume management utilities such as LVM2 and dmraid.

The device-mapper packages have been upgraded to upstream version 1.02.67, which provides a number of bug fixes and enhancements over the previous version. (BZ#746300)

Bug Fix

BZ#454618

The dmeventd daemon was not properly restarted after the package update. Consequently, dmeventd did not apply the newly updated libraries and continued using the old libraries. Therefore, logical volume monitoring failed and had to be re-activated because particular monitoring events were not handled as expected. With this update, dmeventd properly restarts after the package update so that updated libraries are applied and logical volumes are monitored as expected.

Users are advised to upgrade to these updated device-mapper packages, which fix these bugs and add these enhancements.

4.32. device-mapper-multipath

4.32.1. RHBA-2011:1483 — device-mapper-multipath bug fix update

Updated device-mapper-multipath packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The device-mapper-multipath packages provide tools to manage multipath devices by using the device-mapper multipath kernel module, as well as by creating and removing partitions for Device-Mapper devices.

Bug Fix

BZ#729478

The multipath priority callout programs did not work correctly with CCISS (Compaq Command Interface for SCSI-3 Support) devices because the multipath utility was not able to convert the "!" character in the CCISS sysfs name to the "/" character in the CCISS device name. As a consequence, callout programs failed to set path priorities for these devices. The underlying code has been modified, and the multipath utility now supports the new "%c" wildcard for callout functions, and thus ensures the correct CCISS names conversion.

All users of device-mapper-multipath are advised to upgrade to these updated packages, which fix this bug.

4.32.2. RHBA-2011:1152 — device-mapper-multipath bug fix update

Updated device-mapper-multipath packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The device-mapper-multipath packages provide tools to manage multipath devices by giving the dm-multipath kernel module instructions on what to do, as well as by managing the creation and removal of partitions for Device-Mapper devices.

Bug Fix

BZ#728144

Previously, device-mapper-multipath was looking for a CCISS device information at the incorrect location in the sysfs file system. As a consequence, it was impossible to configure multipath on CCISS devices. This bug has been fixed, device-mapper-multipath now finds the device information properly in the described scenario, and multipath can now be properly configured on CCISS devices.

All users of device-mapper-multipath are advised to upgrade to these updated packages, which fix this bug.

4.32.3. RHBA-2012:0166 — device-mapper-multipath bug fix update

Updated *device-mapper-multipath* packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

The *device-mapper-multipath* packages provide tools for managing of multipath devices using the device-mapper multipath kernel module.

Bug Fixes

BZ#741664

If a multipath device was deleted while its path was being checked, the **multipathd** daemon did not abort the path check. Consequently, the **multipath** application terminated unexpectedly if it attempted to access the multipath device information. With this update, **multipathd** aborts the path check and the daemon no longer crashes in this scenario.

BZ#703501

Previously, the **multipathd** daemon was looking for Compaq Command Interface for SCSI-3 Support (CCISS) device information at an incorrect location in the **sysfs** file system. As a

consequence, it was impossible to configure multipath on CCISS device. This bug has been fixed, device-mapper-multipath now finds the device information in the described scenario, and multipath can now properly configure CCISS devices.

BZ#702410

The **multipathd** daemon was printing warning messages on removal of non-multipath Device Mapper devices. With this update, the underlying code has been fixed and no warning messages are logged on removal of such devices.

BZ#737072

Previously, SCSI targets could time out on SCSI commands and consequently become unresponsive. This happened because the **mpath_prio_alua** priority callout used by the commands was set to five minutes. With this update, the callout timeout has been changed to one minute.

BZ#703277

The **multipathd** daemon maintains a list of essential directories it needs to be able to access from its private namespace at all times. When unmounting an unnecessary device, multipath checks if the device mount point is not in the list. Previously, **multipathd** did not check whether the directories listed were symbolic links to the devices and did not consider the devices mounted at the symlinked mount point to be necessary. Consequently, if such a device was marked as unnecessary, multipathd unmounted the device even though the location was listed as essential, because it was listed as a symbolic link. With this update, multipathd detects symbolic links to necessary devices in the list and the symlinked devices are not unmounted. This update also adds a new parameter, ***keep_dir***, which allows users to specify directories that multipathd preserves in its private namespace.

BZ#655203

If the user attempted to delete a multipath device but failed because partitions of the device were in use, some of the device partitions remained deleted. With this update, if **multipathd** fails to delete the entire device, it restores any partitions, which were already deleted.

BZ#729478

The multipath priority callout programs did not work correctly with CCISS (Compaq Command Interface for SCSI-3 Support) devices because the multipath utility was not able to convert the exclamation mark (**!**) character in the CCISS **sysfs** name to the slash (**/**) character in the CCISS device name. As a consequence, the callout programs failed to set path priorities for these devices. The multipath utility now supports the new **%c** wildcard for callout functions and the CCISS names are converted correctly.

BZ#650795

The **multipathd** daemon returned incorrect path groupings for the multipath devices configured to use the group_by_node_name grouping policy. This was due to an incorrect reporting of the target node name for iSCSI targets. With this update, **multipath** checks the iSCSI target name if the FC (Fibre Channel) path check fails and the target name reporting works as expected.

BZ#716329

Previously, **multipathd** terminated unexpectedly if the ***file_timeout*** parameter was set to **0**. With this update, multipathd uses the default file timeout of 90 seconds just as when the parameter is set to a negative value and the problem no longer occurs.

BZ#740512

The **mpath_prio_alua** callout occasionally failed. This happened because **multipathd** did not clean some of the buffers used to collect the SCSI data. With this update, the buffers are cleaned properly and the problem no longer occurs.

BZ#740022

Multipath commands failed on a multipath device if the current working directory contained a file with the same name as the multipath device name. This happened because **multipathd** assumed that the argument was referring to the file. Multipath now performs a check to prevent such an incorrect argument handling and the commands are executed as expected in this scenario.

BZ#655976

On a device set to **manual** failback, multipath was incorrectly failed back to the primary path group on a path's priority change. With this update, the device no longer fails back to the primary path group under these circumstances.

BZ#711970

Previously, the multipath default configuration defined the path selector using the **selector** key word, while device sections were using the **path_selector** key word. To ensure consistency, the default section now accepts both key words, the **selector** and **path_selector**.

BZ#719575

The **kpartx** utility built partition devices for GUID partition tables (GPT) with incorrect partition entry size. This happened because the utility did not validate the size of the GUID partitions. The **kpartx** utility now checks the size of the partitions, and partitions of an invalid GPT are no longer created.

BZ#715524

Previously, the default config value **file_timeout** was not documented. This update adds the respective documentation to the **multipath.conf.annotated** file.

All *device-mapper-multipath* users are advised to upgrade to these updated packages, which fix these bugs.

4.33. dhcp

4.33.1. RHSA-2011:1160 — Moderate: dhcp security update

Updated dhcp packages that fix two security issues are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The Dynamic Host Configuration Protocol (DHCP) is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address.

Security Fixes

CVE-2011-2748, **CVE-2011-2749**

Two denial of service flaws were found in the way the dhcpd daemon handled certain incomplete request packets. A remote attacker could use these flaws to crash dhcpd via a specially-crafted request.

Users of DHCP should upgrade to these updated packages, which contain a backported patch to correct these issues. After installing this update, all DHCP servers will be restarted automatically.

4.33.2. RHBA-2012:0194 — dhcp bug fix update

Updated dhcp packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The Dynamic Host Configuration Protocol (DHCP) is a protocol that allows individual devices on an Internet Protocol (IP) network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address.

Bug Fix

BZ#736515

Previously, the anaconda dhcptimeout value was not fully propagated to libdhcp4client's internal timeout_arg. As a result, it used the insufficient default timeout of 60 seconds. With this update, anaconda dhcptimeout value is correctly propagated and the problem no longer occurs with this update. This update is a dependency of BZ#737155 and BZ#737161.

All DHCP Users are advised to upgrade to these updated packages, which fix this bug.

4.34. dovecot

4.34.1. RHSA-2011:1187 — Moderate: dovecot security update

Updated dovecot packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

Dovecot is an IMAP server for Linux, UNIX, and similar operating systems, primarily written with security in mind.

Security Fix

CVE-2011-1929

A denial of service flaw was found in the way Dovecot handled NULL characters in certain header names. A mail message with specially-crafted headers could cause the Dovecot child process handling the target user's connection to crash, blocking them from downloading the message successfully and possibly leading to the corruption of their mailbox.

Users of dovecot are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the updated packages, the dovecot service will be restarted automatically.

4.35. ecryptfs-utils

4.35.1. RHSA-2011:1241 — Moderate: ecryptfs-utils security update

Updated ecryptfs-utils packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

eCryptfs is a stacked, cryptographic file system. It is transparent to the underlying file system and provides per-file granularity. eCryptfs is released as a Technology Preview for Red Hat Enterprise Linux 5 and 6.

Security Fixes

CVE-2011-1831

The setuid mount.ecryptfs_private utility allows users to mount an eCryptfs file system. This utility can only be run by users in the "ecryptfs" group.

A race condition flaw was found in the way mount.ecryptfs_private checked the permissions of a requested mount point when mounting an encrypted file system. A local attacker could possibly use this flaw to escalate their privileges by mounting over an arbitrary directory.

CVE-2011-1832

A race condition flaw in umount.ecryptfs_private could allow a local attacker to unmount an arbitrary file system.

CVE-2011-1834

It was found that mount.ecryptfs_private did not handle certain errors correctly when updating the mtab (mounted file systems table) file, allowing a local attacker to corrupt the mtab file and possibly unmount an arbitrary file system.

CVE-2011-1835

An insecure temporary file use flaw was found in the ecryptfs-setup-private script. A local attacker could use this script to insert their own key that will subsequently be used by a new user, possibly giving the attacker access to the user's encrypted data if existing file permissions allow access.

CVE-2011-1837

A race condition flaw in mount.ecryptfs_private could allow a local attacker to overwrite arbitrary files.

CVE-2011-3145

A race condition flaw in the way temporary files were accessed in mount.ecryptfs_private could allow a malicious, local user to make arbitrary modifications to the mtab file.

CVE-2011-1833

A race condition flaw was found in the way mount.ecryptfs_private checked the permissions of the directory to mount. A local attacker could use this flaw to mount (and then access) a directory they would otherwise not have access to. Note: The fix for this issue is incomplete until a kernel-space change is made. Future Red Hat Enterprise Linux 5 and 6 kernel updates will correct this issue.

Red Hat would like to thank the Ubuntu Security Team for reporting these issues. The Ubuntu Security Team acknowledges Vasiliy Kulikov of Openwall and Dan Rosenberg as the original reporters of CVE-2011-1831, CVE-2011-1832, and CVE-2011-1833; Dan Rosenberg and Marc Deslauriers as the original reporters of CVE-2011-1834; Marc Deslauriers as the original reporter of CVE-2011-1835; and Vasiliy Kulikov of Openwall as the original reporter of CVE-2011-1837.

Users of ecryptfs-utils are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

4.35.2. RHBA-2011:1503 — ecryptfs-utils bug fix update

Updated ecryptfs-utils packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

eCryptfs is a stacked, cryptographic file system. It is transparent to the underlying file system and provides per-file granularity.

eCryptfs is released as a Technology Preview for Red Hat Enterprise Linux 5.8.

Bug Fixes

BZ#554740

Previously, the eCryptfs daemon, ecryptfsd, failed to start if the ecryptfs kernel module had not already created the files necessary for user space communication under the /dev/ and /dev/misc/ directories, and "No such file or directory" messages were logged. This update avoids this race condition by ensuring that the ecryptfsd daemon waits and then attempts to start again if it discovers that the requisite files have not yet been created.

BZ#553629

Prior to this update ecryptfs did not correctly handle the salt option together with the password file. As a result mounting of the encrypted file system would fail and the error, "Bad address", would be displayed. With this update ecryptfs correctly handles the salt option and mounting of the encrypted file system using eCryptfs no longer fails.

All users of ecryptfs-utils are advised to upgrade to these updated packages, which fix these bugs.

4.36. esound

4.36.1. RHBA-2012:0295 — esound bug fix update

An updated esound package that fixes one bug is now available for Red Hat Enterprise Linux 5.

ESounD, the Enlightened Sound Daemon, is a server process that mixes several audio streams for playback by a single audio device.

Bug Fix

BZ#733090

United States Government Configuration Baseline (USGCB) for Red Hat Enterprise Linux prohibits world-writable directories owned by users. The previous version of ESounD created a temporary directory, /tmp/.esd, with incorrect permissions and placed its socket there. This update ensures that the directory is owned by the root user, and ESounD is thus compliant with the USGCB guidance for Red Hat Enterprise Linux.

All users of esound are advised to upgrade to this updated package, which fixes this bug.

4.37. fcoe-utils

4.37.1. RHBA-2012:0230 — fcoe-utils package update

An updated fcoe-utils package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The fcoe-utils package provides Fibre Channel over Ethernet (FCoE) utilities, such as the fcoeadm command line tool for configuring FCoE interfaces, and the fcoemon service to configure DCB Ethernet QOS filters.

Bug Fixes

BZ#512938

Prior to this update, fcoeadm displayed misleading messages when working with non-existing interfaces. This update modifies the underlying code so that fcoeadm now reports only that no host was found on the interface.

BZ#703374

Prior to this update, the long options "--interface" and "--target" did not report all FCoE instances that were created on the system. This update modifies the commands so that they report all FCoE instances and behave in the same way as the short options "-i" and "-t".

All users of fcoe-utils are advised to upgrade to this updated package, which fixes these bugs.

4.38. fetchmail

4.38.1. RHBA-2011:1540 — fetchmail bug fix update

An updated fetchmail package that fixes a bug is now available for Red Hat Enterprise Linux 5.

Fetchmail is a remote mail retrieval and forwarding utility intended for use over on-demand TCP/IP links, like SLIP or PPP connections.

Bug Fix

BZ#620640

Previously, fetchmail would fail with a socket error when attempting to write to a BSMTP (Batch Simple Mail Transport Protocol) batch file when downloading mail. It failed with a socket error after writing the first header to the BSMTP batch file and displayed, "socket error while fetching from". As a result, fetchmail could not download mail using BSMTP. With this update to fetchmail, the fetchmail package will now correctly write to the BSMTP batch file.

All users of fetchmail are advised to upgrade to this updated package, which resolves this issue.

4.39. file

4.39.1. RHBA-2012:0201 — file bug fix update

Updated file packages that fix various bugs are now available for Red Hat Enterprise Linux 5.

The File utility is used to identify a particular file according to the type of data contained in the file.

Bug Fixes

BZ#486328

Previously, the file utility always checked a section of the core file which was only used by FreeBSD when looking up command names. As a consequence, an incorrect command name could be reported. This update checks this offset only if the core file was generated on a FreeBSD plattfrom. Now, the file utility displays the correct file name.

BZ#489493

Previously, the file utility did not correctly recognize file system dumps generated by the "dump" utility on PowerPC and IBM System z platforms which were wrongly identified as a "JVT NAL" sequence. This update modifies the order of the magic patterns. Now, the file utility correctly identifies these dumps.

BZ#494831

Previously, the Note field stored in Executable and Linkable Format (ELF) binaries was wrongly processed twice. As a consequence, the message "for GNU/Linux X.Y.Z" was displayed twice for certain binary files. This update modifies the process. Now, the Note field is processed only once.

BZ#498671

Previously, the definition for the Multipurpose Internet Mail Extensions (MIME) type "XML" was missing in the magic file. As a consequence, the MIME type for XML files was not displayed. This update adds this MIME type to the magic file.

BZ#504417

Previously, the file utility did not recognize the swap file system on PowerPC platforms. Now, a new magic pattern for swap on PowerPC platforms is added and the file utility now identifies the

swapspace correctly.

BZ#505656

Previously, the "msword" MIME type was listed two times in DOC/XLS magic patterns. As a consequence, the "application/msword" MIME type was displayed twice for certain Microsoft Office 2007 files. Now, the second MIME type definition is removed.

BZ#508688

Previously, the magic pattern for detecting the PPD files did not work as expected. As a consequence, the file utility truncated the "version" string of certain PPD files. This update displays the "version" string correctly and no longer truncates the version number.

BZ#548450

Previously, the manual page did not mention that a 0 exit code was returned when input files were not found. This update adds the missing information to the manual page.

BZ#618910

Previously, the file utility always attempted to read complete files from stdin to get additional information about ELF binary even when the file was not an ELF binary. As a consequence, the process used a large amount of memory and took a long time. This update detects if a file is an ELF binary using the ELF magic bytes and reads the complete file only when the file is an ELF binary.

BZ#641838

Previously, the file utility could wrongly recognize gzip files as FLC files. This update changes the order of gzip and FLC magic patterns. Now, the file utility identifies gzip files correctly.

BZ#668125

Previously, the GFS1 and GFS2 file systems shared the same magic number in the superblock which the file utility used to identify the GFS2 file system. As a consequence, the file utility wrongly recognized GFS2 file systems as GFS1 file systems. This update adds a new magic pattern for the GFS2 file system. Now, the file utility identifies GFS2 correctly.

BZ#692435

Previously, two magic patterns for XML identification were wrongly merged into one. As a consequence, the file utility could not identify the MIME type for XML files starting with "?xml". This update splits these two patterns. Now, the correct MIME type is displayed.

BZ#758429

Previously, the file utility could wrongly recognize JPEG files as Minix file systems. This update changes the order of JPEG and Minix magic patterns. Now the file utility recognizes JPEG files correctly.

All users of the file utility are advised to upgrade to these updated packages, which fix these bugs.

4.40. firefox

4.40.1. RHSA-2012:0079 — Critical: firefox security update

Updated firefox packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2011-3659

A use-after-free flaw was found in the way Firefox removed nsDOMAttribute child nodes. In certain circumstances, due to the premature notification of AttributeChildRemoved, a malicious script could possibly use this flaw to cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0442

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0444

A flaw was found in the way Firefox parsed Ogg Vorbis media files. A web page containing a malicious Ogg Vorbis media file could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0449

A flaw was found in the way Firefox parsed certain Scalable Vector Graphics (SVG) image files that contained eXtensible Style Sheet Language Transformations (XSLT). A web page containing a malicious SVG image file could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2011-3670

The same-origin policy in Firefox treated http://example.com and http://[example.com] as interchangeable. A malicious script could possibly use this flaw to gain access to sensitive information (such as a client's IP and user e-mail address, or httpOnly cookies) that may be included in HTTP proxy error replies, generated in response to invalid URLs using square brackets.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.6.26:

http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.26

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.6.26, which

corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.40.2. RHSA-2011:1437 — Critical: firefox security update

Updated firefox packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2011-3647

A flaw was found in the way Firefox handled certain add-ons. A web page containing malicious content could cause an add-on to grant itself full browser privileges, which could lead to arbitrary code execution with the privileges of the user running Firefox.

CVE-2011-3648

A cross-site scripting (XSS) flaw was found in the way Firefox handled certain multibyte character sets. A web page containing malicious content could cause Firefox to run JavaScript code with the permissions of a different website.

CVE-2011-3650

A flaw was found in the way Firefox handled large JavaScript scripts. A web page containing malicious JavaScript could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.6.24:

http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.24

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.6.24, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.40.3. RHSA-2011:1341 — Critical: firefox security update

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2011-2995

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2011-2372

A flaw was found in the way Firefox processed the "Enter" keypress event. A malicious web page could present a download dialog while the key is pressed, activating the default "Open" action. A remote attacker could exploit this vulnerability by causing the browser to open malicious web content.

CVE-2011-3000

A flaw was found in the way Firefox handled Location headers in redirect responses. Two copies of this header with different values could be a symptom of a CRLF injection attack against a vulnerable server. Firefox now treats two copies of the Location, Content-Length, or Content-Disposition header as an error condition.

CVE-2011-2999

A flaw was found in the way Firefox handled frame objects with certain names. An attacker could use this flaw to cause a plug-in to grant its content access to another site or the local file system, violating the same-origin policy.

CVE-2011-2998

An integer underflow flaw was found in the way Firefox handled large JavaScript regular expressions. A web page containing malicious JavaScript could cause Firefox to access already freed memory, causing Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.6.23:

http://www.mozilla.org/security/known-vulnerabilities/firefox36.html#firefox3.6.23

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.6.23, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.40.4. RHSA-2011:1268 — Important: firefox security update

Updated firefox packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fix

BZ#735483

The RHSA-2011:1242 Firefox update rendered HTTPS certificates signed by a certain

Certificate Authority (CA) as untrusted, but made an exception for a select few. This update removes that exception, rendering every HTTPS certificate signed by that CA as untrusted.

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.6.22. After installing the update, Firefox must be restarted for the changes to take effect.

4.40.5. RHSA-2011:1242 — Important: firefox security update

Updated firefox packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fix

BZ#734316

It was found that a Certificate Authority (CA) issued a fraudulent HTTPS certificate. This update renders any HTTPS certificates signed by that CA as untrusted, except for a select few. The now untrusted certificates that were issued before July 1, 2011 can be manually re-enabled and used again at your own risk in Firefox; however, affected certificates issued after this date cannot be re-enabled or used.

All Firefox users should upgrade to these updated packages, which contain a backported patch. After installing the update, Firefox must be restarted for the changes to take effect.

4.40.6. RHSA-2011:1164 — Critical: firefox security update

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2011-2982

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2011-0084

A dangling pointer flaw was found in the Firefox Scalable Vector Graphics (SVG) text manipulation routine. A web page containing a malicious SVG image could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2011-2378

A dangling pointer flaw was found in the way Firefox handled a certain Document Object Model (DOM) element. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2011-2981

A flaw was found in the event management code in Firefox. A website containing malicious JavaScript could cause Firefox to execute that JavaScript with the privileges of the user running Firefox.

CVE-2011-2983

A flaw was found in the way Firefox handled malformed JavaScript. A web page containing malicious JavaScript could cause Firefox to access already freed memory, causing Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2011-2984

It was found that a malicious web page could execute arbitrary code with the privileges of the user running Firefox if the user dropped a tab onto the malicious web page.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 3.6.20. You can find a link to the Mozilla advisories in the References section of this erratum.

All Firefox users should upgrade to these updated packages, which contain Firefox version 3.6.20, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.41. firstboot

4.41.1. RHBA-2012:0278 — firstboot bug fix update

Updated firstboot packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

The firstboot utility runs after system installation and guides the user through a series of steps that allows for easier configuration of the machine.

Bug Fixes

BZ#642510

Previously, the number of active sound cards was counted incorrectly. As a consequence, even if no sound cards were installed, the sound setup screen could be displayed after the user had set up an account. With this update, the number of active sound cards is counted correctly, and the sound card screen is now displayed only if supported hardware is found.

BZ#653442, BZ#706074

On architectures where the firstboot utility is supported to run only in text mode, firstboot could fail to start with a traceback if the DISPLAY environment variable was set. With this update, an error message is displayed, and informs the user that the firstboot-tui utility can not be run when DISPLAY is set. In addition, users are advised to install the firstboot package, which provides the firstbootWindow.py file and fixes the problem.

All users of firstboot are advised to upgrade to these updated packages, which fix these bugs.

4.42. foomatic

4.42.1. RHSA-2011:1109 — Moderate: foomatic security update

An updated foomatic package that fixes one security issue is now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

Foomatic is a comprehensive, spooler-independent database of printers, printer drivers, and driver descriptions. The package also includes spooler-independent command line interfaces to manipulate queues and to print files and manipulate print jobs. foomatic-rip is a print filter written in Perl.

Security Fix

CVE-2011-2697

An input sanitization flaw was found in the foomatic-rip print filter. An attacker could submit a print job with the username, title, or job options set to appear as a command line option that caused the filter to use a specified PostScript printer description (PPD) file, rather than the administrator-set one. This could lead to arbitrary code execution with the privileges of the "lp" user.

All foomatic users should upgrade to this updated package, which contains a backported patch to resolve this issue.

4.43. freeipmi

4.43.1. RHBA-2011:1499 — freeipmi bug fix update

Updated freeipmi packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The FreeIPMI project provides "Remote-Console" (out-of-band) and "System Management Software" (in-band) based on the Intelligent Platform Management Interface specification.

Bug Fixes

BZ#439411

Prior to this update, the "ipmi-sel" tool did not properly initialize itself and crashed when reading an empty SEL (System Event Log). With this update, ipmi-sel initialization is fixed and the tool no longer crashes when reading an empty SEL.

BZ#639850

Prior to this update, the "freeipmi-bmc-watchdog" service start did not expect that a Baseboard Management Controller (BMC) watchdog timer could already be running and did not reset the timer. In addition, the service stop did not stop the BMC watchdog timer. This could result in a watchdog timer resetting, or shutting down, the machine. With this update, "service freeipmi-

bmc-watchdog start" resets any previously started BMC watchdog timer and "service freeipmi-bmc-watchdog stop" correctly stops the timer. As a result the machine boots up normally.

All users of freeipmi are advised to upgrade to these updated packages, which fix these bugs.

4.44. freeradius2

4.44.1. RHBA-2012:0196 — freeradius2 bug fix and enhancement update

Updated freeradius2 packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 5.

FreeRADIUS is an open-source Remote Authentication Dial In User Service (RADIUS) server which allows RADIUS clients to perform authentication against the RADIUS server. The RADIUS server may optionally perform accounting of its operations via the RADIUS protocol.

The freeradius2 packages have been upgraded to upstream version 2.1.12, which provides a number of bug fixes and enhancements over the previous version. (BZ#609633)

Bug Fixes

BZ#546583

The documentation of command-line arguments was incomplete and in some cases erroneous; some commands did not have a man page. The man pages and help output were updated to correct these deficiencies.

BZ#602567

Previously, freeradius2 did not respect the core dump configuration flag. Consequently, the radiusd process did not produce a core dump file when it terminated unexpectedly with a segmentation fault. With this update the problem has been fixed, and now if radiusd aborts, a core dump is now generated if the core dump flag is enabled.

BZ#658508

The freeradius-pam-conf configuration file, /etc/pam.d/radiusd, referenced a non-existent pam configuration "password-auth". This has been fixed to refer to "system-auth".

BZ#756442

The previous version of freeradius generated its temporary SSL certificates the first time the server was run with the "-X" debug flag. Now the temporary certificates are created the first time the freeradius RPM is installed. It is no longer necessary to run the server in debug mode to create the initial certificates.

BZ#760193

The radtest command-line argument to request the PPP hint option was not parsed correctly. Consequently, radclient did not add the PPP hint to the request packet and the test failed. This update corrects the problem and radtest now functions as expected.

Enhancements

BZ#630072

The radtest tool did not send a Message-Authenticator by default in an Access-Request. Consequently, radtest could not connect to a RADIUS server if it required the authenticator as per RFC 5080. With this update the problem has been fixed, and now the Message-Authenticator is always sent.

Users are advised to upgrade to these updated freeradius2 packages, which fix these bugs and add this enhancement.

4.45. freetype

4.45.1. RHSA-2011:1455 — Important: freetype security update

Updated freetype packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

FreeType is a free, high-quality, portable font engine that can open and manage font files. It also loads, hints, and renders individual glyphs efficiently. The freetype packages for Red Hat Enterprise Linux 4 provide both the FreeType 1 and FreeType 2 font engines. The freetype packages for Red Hat Enterprise Linux 5 and 6 provide only the FreeType 2 font engine.

Security Fixes

CVE-2011-3439

Multiple input validation flaws were found in the way FreeType processed CID-keyed fonts. If a specially-crafted font file was loaded by an application linked against FreeType, it could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

Note

These issues only affected the FreeType 2 font engine.

Users are advised to upgrade to these updated packages, which contain a backported patch to correct these issues. The X server must be restarted (log out, then log back in) for this update to take effect.

4.45.2. RHSA-2011:1402 — Important: freetype security update

Updated freetype packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

FreeType is a free, high-quality, portable font engine that can open and manage font files. It also loads, hints, and renders individual glyphs efficiently. The freetype packages for Red Hat Enterprise Linux 4 provide both the FreeType 1 and FreeType 2 font engines. The freetype packages for Red Hat Enterprise Linux 5 and 6 provide only the FreeType 2 font engine.

Security Fixes

CVE-2011-3256

Multiple input validation flaws were found in the way FreeType processed bitmap font files. If a specially-crafted font file was loaded by an application linked against FreeType, it could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

Note

These issues only affected the FreeType 2 font engine.

Users are advised to upgrade to these updated packages, which contain a backported patch to correct these issues. The X server must be restarted (log out, then log back in) for this update to take effect.

4.46. gamin

4.46.1. RHBA-2011:1537 — gamin bug fix update

Updated gamin packages that fix one bug are now available for Red Hat Enterprise Linux 5.

Gamin is an implementation of a subset of the File Alteration Monitor (FAM). It is both API and ABI compatible with the file alteration monitoring mechanism, but does not depend on a system-wide daemon.

Bug Fix

BZ#503085

Due to an assertion check, the Gamin server terminated unexpectedly after a certain amount of time. With this update, the assertion has been silenced so that the Gamin server now works as expected.

All users are advised to upgrade to these updated gamin packages, which fix this bug.

4.47. gawk

4.47.1. RHBA-2011:1486 — gawk bug fix update

An updated gawk package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The gawk package contains the GNU version of awk, a text processing utility. Awk interprets a special-purpose programming language to do quick and easy text pattern matching and reformatting jobs.

Bug Fix

BZ#629196

Prior to this update gawk interpreted (under certain circumstances) some run-time variables as internal zero-length variable prototypes. When gawk tried to free such run-time variables, it actually freed the internal prototypes, that were allocated just once due to memory savings. Consequently gawk sometimes failed and the error message "awk: double free or corruption" was displayed. With this update the problem has been corrected and the error no longer occurs.

All users of gawk are advised to upgrade to this updated package, which fixes this bug.

4.48. gcc

4.48.1. RHBA-2012:0258 — gcc bug fix update

Updated gcc packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

The gcc packages provide compilers for C, C++, Java, Fortran, Objective C, and Ada 95 GNU, as well as related support libraries.

Bug Fixes

BZ#651098

Previously, the g++ compiler consumed excessive memory when compiling a program that used a vast amount of various data definitions and function overloading. This has been fixed and the g++ compiler uses much less memory under these circumstances.

BZ#745004

Global variable lookup did not match the C code lookup. As a result, a variable appeared to have incorrect values assigned during debugging. This happened if a global variable with the same name was exported by multiple libraries and the libraries were stored at the same location. With this update, the variable lookup has been modified to match the C code lookup.

BZ#706383

The gcov tool incorrectly counted opening brackets in an error handling block specification ("throw") if the specification was not located on the same line as its parent function. With this update, the code handling for such situations has been added and the throw blocks are handled as expected.

BZ#735304

A program compilation could terminate with an internal compiler error because the compiler failed to update hash tables while creating precompiled headers of the libstdc++ library. With this update, the compiler uses the DECL_UID variable when creating the precompiled headers and the problem no longer occurs.

BZ#722252

A GNU Data Language (GDL) program compilation could terminate with an internal compiler error. This happened due to incorrect gimplification of the try-catch block. With this update, the underlying code has been modified and the try-catch blocks are now compiled correctly.

BZ#746405

Under certain circumstances, program compilation with the gfortran compiler could have resulted in the following error:

internal compiler error: in modified_type_die, at dwarf2out.c:8495

With this update, the underlying code has been modified and the problem no longer occurs.

All gcc users are advised to upgrade to these updated packages, which fix these bugs.

4.49. gcc44

4.49.1. RHEA-2012:0272 — gcc44 enhancement update

Updated gcc44 packages that add one enhancement are now available for Red Hat Enterprise Linux 5.

The gcc44 packages provide the GNU Compiler Collection (GCC), which includes GNU compilers and related support libraries for C, C++, and Fortran programming languages. These packages also include libgomp, the GNU implementation of the OpenMP Application Programming Interface for multi-platform shared-memory parallel programming.

Enhancement

BZ#742118

This update adds binutils for the AMD FX Bulldozer central processing unit (CPU) to support the Bulldozer-capable gcc44 toolchain.

All users of gcc44 are advised to upgrade to these updated gcc44 packages, which add this enhancement.

4.50. gdb

4.50.1. RHBA-2011:1129 — gdb bug fix update

An updated gdb package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The GNU Debugger (GDB) allows debugging of programs written in C, C++, Java, and other languages by executing them in a controlled fashion and then printing out their data.

Bug Fix

BZ#728151

When the GDB convenience variable contained a structure, accessing a field of this structure caused a GDB internal error. The code has been modified to ensure that internal setting of field address is not executed for GDB convenience variables. As result, GDB can now access fields of structures stored in convenience variables.

All users of gdb are advised to upgrade to this updated package, which resolves this issue.

4.50.2. RHBA-2012:0238 — gdb bug fix update

An updated gdb package that fixes multiple bugs is now available for Red Hat Enterprise Linux 5.

The GNU Debugger (GDB) allows users to debug programs written in C, C++, and other languages by executing them in a controlled fashion and then printing out their data.

Bug Fixes

BZ#658851

GDB could stop with an error when trying to access the libpthread shared library before the library was relocated. With this update, GDB lets the library relocations be resolved first, allowing GDB to debug programs properly under these circumstances.

BZ#696148

Modifying a string in the executable using the "-write" command line option could fail with an error if the executable was not running. With this update, GDB can modify executables even before they are started.

BZ#720717

When printing data from a string buffer of constant size, GDB, by default, also prints the data following after the first zero byte ("\0") of the string. To display only the data before the zero byte, the "set print null-stop" option has to be set. Previously with this option set, GDB did not display any string content due to an incorrect zero byte test condition in the code. The test condition has been corrected and GDB now properly displays data located before the first zero byte.

BZ#727726

GDB convenience variables allow a user to store and retrieve arbitrary data of arbitrary data types. Previously, when the GDB convenience variable contained a structure data type, accessing a field of the structure caused an internal error. With this update, this problem has been corrected, and GDB now works with structure convenience variables correctly.

BZ#748267

When loading a core dump file for debugging, GDB could incorrectly interpret inappropriate memory content as the pthread_t identifier if the version of the glibc library installed on the system did not match the glibc version used to create the core dump file. Consequently, initialization of the libthread_db library failed due to an unexpected value of pthread_t, which led to a GDB internal error. With this update, GDB only displays a warning message and successfully loads the core file. Instead of the pthread_t identifiers, which are unavailable in this failure scenario, GDB displays the LWP (light-weight process) identifiers that match the Linux TID (Thread Identifier) values of the threads found in the core file.

All GDB users are advised to upgrade to this updated package, which fixes these bugs.

4.51. gdm

4.51.1. RHBA-2012:0282 — gdm bug fix update

Updated gdm packages that fix three bugs are now available for Red Hat Enterprise Linux 5.

The GNOME Display Manager (GDM) is a highly configurable reimplementation of XDM, the X Display Manager. GDM allows you to log into your system with the X Window System running and supports running several different X sessions on your local machine at the same time.

Bug Fixes

BZ#217417

Previously, the gdmsetup utility did not automatically add users to the user whitelist file /etc/gdm/custom.conf, although these users were configured for automatic login. With this update, the problem has been fixed and users are now automatically added to the whitelist file, as expected.

BZ#575771

Previously, the GDM GUI was not properly resized when the failed authentication message was displayed for the user. As a result, the failed authentication message was not displayed correctly. With this update, the problem has been fixed so that the GUI is resized properly and the message is displayed as expected.

BZ#658506

When shutting down the X Window System, the gdm-rh-security-token-helper program could have terminated unexpectedly with a segmentation fault under certain circumstances. With this update, the problem has been fixed, and gdm-rh-security-token-helper works as expected.

All users of GDM are advised to upgrade to these updated packages, which fix these bugs.

4.52. gfs-kmod

4.52.1. RHBA-2012:0277 — gfs-kmod bug fix update

Updated gfs-kmod packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

The gfs-kmod packages contain kernel modules that provide the ability to mount and use the Global File System (GFS).

Bug Fixes

BZ#732129

Previously, the directory pre-fetching GFS functionality could decrease performance of some applications that were running on the GFS file system. This update introduces a new GFS mounting option, "-o noprefetch", which disables the directory pre-fetching feature. The applications running on the GFS file system mounted with this option no longer experience performance problems caused by this feature.

BZ#761157

When attempting to add files to a GFS file system and the file system became full, the GFS kernel daemon did not properly release resources allocated for inodes that could not be created. This could result in file system corruption. This patch introduces new cleanup code, which removes partially created inodes and releases allocated resources correctly.

All users of gfs-kmod are advised to upgrade to these updated packages, which fix these bugs.

4.53. gfs-utils

4.53.1. RHBA-2012:0276 — gfs-utils bug fix update

An updated gfs-utils package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The gfs-utils package provides various user-space tools necessary to mount, create, maintain, and test Global File Systems (GFS).

Bug Fixes

BZ#704328

Prior to this update, metawalk.c did not correctly consider leaf continuation blocks. As a result, the offline GFS file system checker (gfs_fsck) did not correctly check file systems with 500,000 or more files. This update modifies the fsck.gfs code so that gfs_fsck now also works on larger file systems.

BZ#766646

Prior to this update, the gfs_mount(8) manual page did not list the recently added the GFS mount options "-o noprefetch", "prefetch", "errors=panic", and "errors=withdraw". This update adds these GFS mount options.

All users of gfs-utils are advised to upgrade to this updated package, which fixes this bug.

4.54. gfs2-utils

4.54.1. RHBA-2012:0269 — gfs2-utils bug fix and enhancement update

An updated gfs2-utils package that fixes various bugs and adds one enhancement is now available for Red Hat Enterprise Linux 5.

The gfs2-utils package provides the user-space utilities necessary to mount, create, maintain and test GFS2 file systems.

Bug Fixes

BZ#711451

To expand a GFS2 file system, additional resource groups must be added to manage new space. The gfs2_grow utility ensures this by writing to the rindex file. Previously, if there was not enough free space in the file system to write out new resource group entries, gfs2_grow was unable to update the rindex file. As a consequence, gfs2_grow was unable to expand the file system and failed with the following error message:

Error writing new rindex entries;aborted.

With this update, gfs2_grow writes one resource group at first, and then the rest instead of attempting to write all the new resource groups at once. Now, gfs2_grow successfully expands the file system in the described scenario.

BZ#714739

Previously, the libgfs2 library used the obsolete MAJOR() and MINOR() macros to handle device numbers. These macros did not support device numbers greater than 255, and could cause error messages to be displayed when using gfs2-utils. The macros have been replaced by the major() and minor() functions, and gfs2-utils now works properly with device numbers greater than 255.

BZ#720935

Previously, the "mkfs.gfs2" command worked only on block devices. Using the command on sparse files failed with an error message. An upstream patch has been applied to address this issue, and the mkfs.gfs2 utility now also recognizes regular files.

BZ#730091

Previously, the gfs2_grow utility failed to expand a GFS file system if the file system contained only one resource group. This was due to old code based on GFS1 (which had different fields) that calculated distances between resource groups and did not work with only one resource group. This update adds the rgrp_size() function in libgfs2, which calculates the size of the resource group instead of determining its distance from the previous resource group. The file system with only one resource group can now be expanded successfully.

BZ#745126

Due to a bug in libgfs2, sentinel directory entries were counted as if they were real entries. As a consequence, the mkfs.gfs2 utility created file systems which did not pass the fsck check when a large number of journal metadata blocks was required (for example, a file system with block size of 512, and 9 or more journals). With this update, incrementing the count of the directory entry is now avoided when dealing with sentinel entries. GFS2 file systems created with large numbers of journal metadata blocks now pass the fsck check cleanly.

Enhancement

BZ#702296

Prior to this update, when executing the "gfs2_edit" command with the "savemeta" or "restoremeta" options specified, the command produced uncompressed files that were very large in size. This update allows gfs2_edit to compress metadata while writing by using the "savemeta" option, and also read a compressed metadata file by using the "restoremeta" option.

All users of gfs2-utils are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.55. ghostscript

4.55.1. RHSA-2012:0095 — Moderate: ghostscript security update

Updated ghostscript packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are

available for each vulnerability from the CVE links associated with each description below.

Ghostscript is a set of software that provides a PostScript interpreter, a set of C procedures (the Ghostscript library, which implements the graphics capabilities in the PostScript language) and an interpreter for Portable Document Format (PDF) files.

Security Fixes

CVE-2009-3743

An integer overflow flaw was found in Ghostscript's TrueType bytecode interpreter. An attacker could create a specially-crafted PostScript or PDF file that, when interpreted, could cause Ghostscript to crash or, potentially, execute arbitrary code.

CVE-2010-2055

It was found that Ghostscript always tried to read Ghostscript system initialization files from the current working directory before checking other directories, even if a search path that did not contain the current working directory was specified with the "-I" option, or the "-P-" option was used (to prevent the current working directory being searched first). If a user ran Ghostscript in an attacker-controlled directory containing a system initialization file, it could cause Ghostscript to execute arbitrary PostScript code.

CVE-2010-4820

Ghostscript included the current working directory in its library search path by default. If a user ran Ghostscript without the "-P-" option in an attacker-controlled directory containing a specially-crafted PostScript library file, it could cause Ghostscript to execute arbitrary PostScript code. With this update, Ghostscript no longer searches the current working directory for library files by default.

Note

The fix for CVE-2010-4820 could possibly break existing configurations. To use the previous, vulnerable behavior, run Ghostscript with the "-P" option (to always search the current working directory first).

CVE-2010-4054

A flaw was found in the way Ghostscript interpreted PostScript Type 1 and PostScript Type 2 font files. An attacker could create a specially-crafted PostScript Type 1 or PostScript Type 2 font file that, when interpreted, could cause Ghostscript to crash or, potentially, execute arbitrary code.

Users of Ghostscript are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

4.55.2. RHBA-2011:1286 — ghostscript bug fix update

An updated ghostscript package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The Ghostscript suite provides a PostScript(TM) interpreter, a set of C procedures (the Ghostscript library, which implements the graphics capabilities in the PostScript language), and an interpreter for

PDF files. Ghostscript translates PostScript code into many common, bitmapped formats, especially formats understood by most printers and displays. This enables users to display PostScript files and print them on non-PostScript printers.

Bug Fixes

BZ#734764

Prior to this update, the page orientation was incorrect when pages in landscape orientation were converted to the PXL raster format. This update matches landscape page sizes as well as portrait page sizes, and sets the orientation parameter correctly when a match is found.

BZ#734767

Prior to this update, certain input files containing CID Type2 fonts were rendered with incorrect character spacing. This update modifies the code so that all input files with CID Type2 fonts are rendered correctly.

Users are advised to upgrade to this updated package, which fixes these bugs.

4.55.3. RHBA-2012:0284 — ghostscript bug fix and enhancement update

Updated ghostscript packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 5.

The Ghostscript suite provides a PostScript interpreter, a set of C procedures (the Ghostscript library, which implements the graphics capabilities in the PostScript language), and an interpreter for PDF files. Ghostscript translates PostScript code into many common bitmapped formats like those understood by most printers and displays. This enables users to display PostScript files and print them on non-PostScript printers.

Bug Fixes

BZ#675307

Previously, using the ps2pdf utility to convert a PostScript file to the PDF format caused the resulting document to be created with non-working hyperlinks. This update applies an upstream patch that resolves this issue, and ps2pdf now creates PDF files with correct hyperlinks.

BZ#688996

Prior to this update, certain input files containing CID Type2 fonts were rendered with incorrect character spacing. This update modifies the code so that all input files with CID Type2 fonts are rendered correctly.

BZ#692165

Prior to this update, the page orientation was incorrect when pages in landscape orientation were converted to the PXL raster format. This update matches landscape page sizes as well as portrait page sizes, and sets the orientation parameter correctly when a match is found.

Enhancement

BZ#710074

Improved support for the PDF/A format has been back-ported from upstream.

Users are advised to upgrade to these updated ghostscript packages, which resolve these issues and add this enhancement.

4.56. glibc

4.56.1. RHSA-2012:0126 — Moderate: glibc security update

Updated glibc packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The glibc packages contain the standard C libraries used by multiple programs on the system. These packages contain the standard C and the standard math libraries. Without these two libraries, a Linux system cannot function properly.

Security Fixes

CVE-2009-5029

An integer overflow flaw, leading to a heap-based buffer overflow, was found in the way the glibc library read timezone files. If a carefully-crafted timezone file was loaded by an application linked against glibc, it could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2009-5064

A flaw was found in the way the ldd utility identified dynamically linked libraries. If an attacker could trick a user into running ldd on a malicious binary, it could result in arbitrary code execution with the privileges of the user running ldd.

CVE-2010-0830

An integer overflow flaw, leading to a heap-based buffer overflow, was found in the way the glibc library loaded ELF (Executable and Linking Format) files. If a carefully-crafted ELF file was loaded by an application linked against glibc, it could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2011-1089

It was found that the glibc addmntent() function, used by various mount helper utilities, did not handle certain errors correctly when updating the mtab (mounted file systems table) file. If such utilities had the setuid bit set, a local attacker could use this flaw to corrupt the mtab file.

CVE-2011-4609

A denial of service flaw was found in the remote procedure call (RPC) implementation in glibc. A remote attacker able to open a large number of connections to an RPC service that is using the RPC implementation from glibc, could use this flaw to make that service use an excessive amount of CPU time.

Red Hat would like to thank the Ubuntu Security Team for reporting CVE-2010-0830, and Dan Rosenberg for reporting CVE-2011-1089. The Ubuntu Security Team acknowledges Dan Rosenberg as the original reporter of CVE-2010-0830.

Users should upgrade to these updated packages, which resolve these issues.

4.56.2. RHBA-2011:1488 — glibc bug fix update

Updated glibc packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The glibc packages provide the standard C and standard math libraries used by multiple programs on the system. Without these libraries, the Linux system cannot function properly.

Bug Fix

BZ#745487

Previously, the dynamic loader generated an incorrect ordering for initialization according to the ELF specification. Initialization routines for depended-upon objects were not being called before the objects, which depended on them, were being initialized. This manifested itself only when initializing compiled C++ libraries whose global initialization depended upon the global initialization of data in other libraries which they were linked against at link time, generating a DT_NEEDED entry. With this update, implementation of the topological sort algorithm for dependency resolution has been fixed, and functions for initialization and termination are now ordered correctly.

All users are advised to upgrade to these updated packages, which fix this bug.

4.56.3. RHBA-2012:0260 — glibc bug fix update

Updated glibc packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

The glibc packages provide the standard C and standard math libraries used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly.

Bug Fixes

BZ#585433

Priviously, glibc incorrectly computed the amount of memory needed by strcoll_l and strxfrm functions. As a consequence, a stack overflow could occur, especially in multi-threaded applications with small stack sizes. This update fixes the memory usage computations and avoids the stack overflows.

BZ#657570

Prior to this update, glibc used an incorrect matching algorithm in the strptime function. As a result, strptime could misparse months in certain locales including Polish and Vietnamese. This update corrects the matching algorithm in strptime.

BZ#675259

Priviously, the glibc locale information was wrong for certain French, Spanish and German locales. As a result, incorrect numeric output could be reported. This update corrects the information.

BZ#678318

Prior to this update, nss_nis client code in glibc attempted to read the passwd.adjunct table for certain usernames. This typically required more privileges than a normal user has and thus errors were logged on the The Network Information Service (NIS) server. This update changes glibc to only refer to passwd.adjunct when it is actually necessary.

BZ#711924

Priviously, the dl_debug_state RT_CONSISTENT incorrectly occurred before applying dynamic relocations. As a result, debugging tools could not correctly monitor this call. This update adds systemtap-probes at a superset of the locations where the dl_debug_state was called.

BZ#711531

Prior to this update, glibc did not initialize the robust futex list after a fork. As a result, shared robust mutexes were not cleaned up when the child exited. This update ensures that the robust futex list is correctly initialized after a fork system call.

BZ#707998

Prior to this update, glibc returned incorrect error codes from the pthread_create. This could lead some programs to incorrectly issue an error for a transient failure, such as a temporary out of memory condition. This update ensures glibc returns the correct error code when memory allocation fails in pthread_create.

BZ#706894

Prior to this update, the system configuration option _SC_NPROCESSORS_CONF returned the total number of active processors configured rather than the total number of configured processors. This update changes glibc to query system configurations to get the number of configured processors correctly.

BZ#703345

Prior to this update, getpwent could incorrectly query NIS when using the nss_compat option. This could lead to incorrect results (missing entries) for calls to getpwent. This update changes glibc to only query the NIS domain when needed.

BZ#729661

Prior to this update, the dynamic loader generated an incorrect ordering for initialization according to the ELF specification. This could result in incorrect ordering of DSO constructors and destructors. With this update, dependency resolution has been fixed

BZ#756453

Prior to this update, the libresolv routines were not compiled with the stack protector enabled. As a consequence, a buffer overflow attack vector could occur if the libresolv routines had potential stack overflows. This update turns on the stack protector mechanisms for libresolv.

BZ#758252

Prior to this update, the futimes function rounded values rather than truncate them. As a consequence, file modification, access, or creation times could be incorrect. This update correctly truncates values and gives the correct file modification, access & creation times.

All users of glibc are advised to upgrade to these updated packages, which fix these bugs.

4.57. Global_File_System

4.57.1. RHBA-2012:0176 — Global_File_System bug fix and enhancement update

Updated Global_File_System packages that fix numerous bugs and add several enhancements are now available for Red Hat Enterprise Linux 5.

The Global File System book provides information about configuring and maintaining Red Hat Global File System for Red Hat Enterprise Linux 5.

The Global File System book has been updated to version 5.8, which provides a number of bug fixes and enhancements over the previous version. (BZ#727325)

All users of the Global File System book are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.58. gnome-screensaver

4.58.1. RHBA-2012:0008 — gnome-screensaver bug fix update

An updated gnome-screensaver package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The gnome-screensaver package contains the GNOME project's official screen saver program. It is designed for improved integration with the GNOME desktop, including themeability, language support, and Human Interface Guidelines (HIG) compliance. It also provides screen-locking and fast user-switching from a locked screen.

Bug Fix

BZ#771849

When locking the screen, the gnome-screensaver application takes exclusive control of the mouse and keyboard. If another application has already taken exclusive control of the keyboard, gnome-screensaver is unable to take over that control. Under these circumstances, gnome-screensaver previously did not engage the screen saver but waited for the keyboard to become available. During this time-frame, the system was unresponsive to mouse clicks because gnome-screensaver held on to control of the mouse. With this update, gnome-screensaver has been modified to release control of the mouse until it can get control of both, the mouse and the keyboard, and the system is no longer unresponsive in this scenario.

All users of gnome-screensaver are advised to upgrade to this updated package, which fixes this bug.

4.58.2. RHBA-2012:0002 — gnome-screensaver bug fix update

An updated gnome-screensaver package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The gnome-screensaver package contains the GNOME project's official screen saver program. It is designed for improved integration with the GNOME desktop, including themeability, language support, and Human Interface Guidelines (HIG) compliance. It also provides screen-locking and fast user-

switching from a locked screen.

Bug Fix

BZ#766799

Previously, gnome-screensaver's PAM configuration file was not marked as a configuration file in the gnome-screensaver spec file, and thus the configuration file was overwritten when updating the gnome-screensaver package. Therefore, after the screen had been locked, users could not log into the system by using some of the previously specified authentication methods, or when users successfully logged in, automatic re-authentication with some applications could fail. With this update, the spec file has been corrected, and the pre-existing gnome-screensaver's PAM configuration file is now preserved when the package is updated so authentication problems no longer occur.

All users of gnome-screensaver are advised to upgrade to this updated package, which fixes this bug.

4.59. gnome-system-monitor

4.59.1. RHBA-2012:0212 — gnome-system-monitor bug fix and enhancement update

An updated gnome-system-monitor package that fixes one bug and adds one enhancement is now available for Red Hat Enterprise Linux 5.

The gnome-system-monitor utility allows users to graphically view and manipulate the running processes on the system, and provides an overview of available resources such as CPU and memory.

Bug Fix

BZ#616487

The previous version of the gnome-system-monitor utility did not close the socket when it terminated, which may have rendered it unable to start for the second time. This update applies a patch that ensures the socket is properly closed when the utility terminates, and gnome-system-monitor now works as expected.

Enhancement

BZ#722866

Previously, the minimum width of the gnome-system-monitor window was limited by the minimum width of its content. Consequently, running this utility on a system with a large number of CPUs caused this window to be very large. This update adds a horizontal scrollbar to make sure the gnome-system-monitor window can fit to the screen even when the system has multiple CPUs.

All users of gnome-system-monitor are advised to upgrade to this updated package, which fixes this bug and adds this enhancement.

4.60. gpart

4.60.1. RHBA-2011:1376 — gpart bug fix update

An updated gpart package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The gpart utility is a small tool, which tries to guess what partitions are on a PC type hard disk in case the primary partition table was damaged.

Bug Fix

BZ#648279

The gpart package was previously only available for the i386 architecture. This update makes the gpart package available for both i386 and 64-bit x86 architectures.

All users of gpart should upgrade to this updated package, which fixes this bug.

4.61. groff

4.61.1. RHBA-2011:1484 — groff bug fix update

Updated groff packages that fix this bug is now available for Red Hat Enterprise Linux 5.

Groff is a document formatting system. Groff takes standard text and formatting commands as input and produces formatted output.

Bug Fix

BZ#448158

Prior to this update groff did not have full path commands in some places and used PATH variables when invoking external binaries. When opening a man page in a restricted shell environment the man page would not be displayed or an erroneous error message, "old character encoding and/or character set", appeared. With this update, groff now uses fully defined paths when invoking external binaries. As a result the man pages can now be displayed in a restricted shell environment.

All users of groff are advised to upgrade to these updated packages, which fixes this bug.

4.62. gtk2

4.62.1. RHBA-2011:1795 — gtk2 bug fix update

An updated gtk2 package that fixes one bug is now available for Red Hat Enterprise Linux 5.

GTK+ is a multi-platform toolkit for creating graphical user interfaces.

Bug Fix

BZ#758019

The GTK+ file chooser did not properly handle the situation of saving a nameless file, which caused GTK+ to become unresponsive. To avoid this problem, an explicit test for this condition has been added in the code, and GTK+ now works as expected.

All users of gtk2 are advised to upgrade to this updated package, which fixes this bug.

4.63. hmaccalc

4.63.1. RHBA-2011:1462 — hmaccalc bug fix update

An updated hmaccalc package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The hmaccalc package contains tools to calculate HMAC (Hash-based Message Authentication Code) values for files. The names and interfaces were designed to mimic those of the sha1sum, sha256sum, sha384sum and sha512sum tools provided by the coreutils package.

Bug Fix

BZ#658178

Prior to this update, hmaccalc erroneously truncated the values which it read from a checkfile before comparing them with the computed values. Consequently, comparison between differently truncated sums of files passed in some cases. This update backports a change which modifies the hmaccalc tool so that when it is used to verify checksums, if it is told to truncate computed values during a verification operation, it will not truncate the values which it reads from a checkfile before comparing them with the computed values. As a result hmaccalc correctly detects differences in hmac values.

All users of hmaccalc are advised to upgrade to this updated package, which fixes this bug.

4.64. httpd

4.64.1. RHSA-2011:1392 — Moderate: httpd security and bug fix update

Updated httpd packages that fix one security issue and one bug are now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The Apache HTTP Server is a popular web server.

Security Fix

CVE-2011-3368

It was discovered that the Apache HTTP Server did not properly validate the request URI for proxied requests. In certain configurations, if a reverse proxy used the ProxyPassMatch directive, or if it used the RewriteRule directive with the proxy flag, a remote attacker could make the proxy connect to an arbitrary server, possibly disclosing sensitive information from internal web servers not directly accessible to the attacker.

Red Hat would like to thank Context Information Security for reporting this issue.

Bug Fix

BZ#736593, BZ#736594

The fix for CVE-2011-3192 provided by the RHSA-2011:1245 update introduced regressions in

the way httpd handled certain Range HTTP header values. This update corrects those regressions.

All httpd users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

4.64.2. RHSA-2011:1245 — Important: httpd security update

Updated httpd packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The Apache HTTP Server is a popular web server.

Security Fix

CVE-2011-3192

A flaw was found in the way the Apache HTTP Server handled Range HTTP headers. A remote attacker could use this flaw to cause httpd to use an excessive amount of memory and CPU time via HTTP requests with a specially-crafted Range header.

All httpd users should upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

4.64.3. RHBA-2012:0261 — httpd bug fix and enhancement update

Updated httpd packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The Apache HTTP Server ("httpd") is the namesake project of The Apache Software Foundation.

Bug Fixes

BZ#700322

In situations when httpd could not allocate memory, httpd sometimes terminated unexpectedly with a segmentation fault rather than terminating the process with an error message. With this update, a patch has been applied to correct this bug and httpd no longer crashes in the scenario described.

BZ#767990

When the "SSLCryptoDevice" config variable in "ssl.conf" was set to an unknown or invalid value, the httpd daemon would terminate unexpectedly with a segmentation fault at startup. With this update the code has been corrected, httpd no longer crashes, and httpd issues an appropriate error message in this scenario.

Enhacements

BZ#677279

The rotatelogs program now provides a new "rotatelogs -c" option to create log files for each set interval, even if empty.

BZ#677288

The rotatelogs program now provides a new "rotatelogs -p" option to execute a custom program after each log rotation.

BZ#709869

The Apache module mod_proxy now allows changing the BalancerMember state in the web interface.

BZ#714725

The Apache module mod_alias now supports redirecting to a local path (that is, a partial URL).

BZ#719907

The Apache module mod_proxy now supports the "connectiontimeout" parameter.

BZ#719941

The httpd service is now automatically restarted after a package upgrade, if the service is running.

Users are advised to upgrade to these updated httpd packages, which fix these bugs and add these enhancements.

4.65. hwdata

4.65.1. RHEA-2012:0235 — hwdata enhancement update

An updated hwdata package that adds various enhancements is now available for Red Hat Enterprise Linux 5.

The hwdata package contains tools for accessing and displaying hardware identification and configuration data.

Enhancements

BZ#711121

The monitor database has been updated with information about Acer 76ie monitors.

BZ#720938

The pci.ids database has been updated with information about future Intel PCH (Platform Controller Hub) devices.

BZ#714098

The pci.ids database has been updated with information about the latest HP iLO4 devices.

BZ#713068

The pci.ids database has been updated with information about future Atheros wireless devices.

BZ#747861

The pci.ids database has been updated according to the latest upstream changes.

All users of hwdata are advised to upgrade to this updated package, which adds these enhancements.

4.66. ibutils

4.66.1. RHSA-2012:0311 — Low: ibutils security and bug fix update

Updated ibutils packages that fix one security issue and one bug are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The ibutils packages provide InfiniBand network and path diagnostics.

Security Fix

CVE-2008-3277

It was found that the ibmssh executable had an insecure relative RPATH (runtime library search path) set in the ELF (Executable and Linking Format) header. A local user able to convince another user to run ibmssh in an attacker-controlled directory could run arbitrary code with the privileges of the victim.

Bug Fix

BZ#711779

Under certain circumstances, the "ibdiagnet -r" command could suffer from memory corruption and terminate with a "double free or corruption" message and a backtrace. With this update, the correct memory management function is used to prevent the corruption.

All users of ibutils are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

4.67. icu

4.67.1. RHSA-2011:1815 — Moderate: icu security update

Updated icu packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The International Components for Unicode (ICU) library provides robust and full-featured Unicode services.

Security Fix

CVE-2011-4599

A stack-based buffer overflow flaw was found in the way ICU performed variant canonicalization for some locale identifiers. If a specially-crafted locale representation was opened in an application linked against ICU, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

All users of ICU should upgrade to these updated packages, which contain a backported patch to resolve this issue. All applications linked against ICU must be restarted for this update to take effect.

4.68. ifd-egate

4.68.1. RHBA-2012:0214 — ifd-egate bug fix update

An updated ifd-egate package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The ifd-egate package provides a smart card reader driver, which enables the PCSC-lite daemon to communicate with Gemalto (formely Axalto) e-gate smart cards.

Bug Fixes

BZ#667126

The ifd-egate package is dependent on the pcsc-lite package but pcsc-lite is not a part of the minimal system installation. Previously, the ifd-egate driver generated a spurious error message when it was installed on the system with minimal installation even though pscs-lite was installed during the same installation transaction. With this update, the spec file has been modified to correct this problem and the error message is no longer generated in this scenario.

BZ#759638

The idf-egate.spec file incorrectly used the "%{dist}" flag instead of the "%{?dist}" flag. With this update, the correct flag is now used.

All users of ifd-egate are advised to upgrade to this updated package, which fixes these bugs.

4.69. ImageMagick

4.69.1. RHSA-2012:0301 — Low: ImageMagick security and bug fix update

Updated ImageMagick packages that fix one security issue and multiple bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

ImageMagick is an image display and manipulation tool for the X Window System that can read and write multiple image formats.

Security Fix

CVE-2010-4167

It was found that ImageMagick utilities tried to load ImageMagick configuration files from the current working directory. If a user ran an ImageMagick utility in an attacker-controlled directory containing a specially-crafted ImageMagick configuration file, it could cause the utility to execute arbitrary code.

Bug Fixes

BZ#502626

Previously, the "identify -verbose" command failed with an assertion if there was no image information available. An upstream patch has been applied, so that GetImageOption() is now called correctly. Now, the "identify -verbose" command works correctly even if no image information is available.

BZ#530592

Previously, an incorrect use of the semaphore data type led to a deadlock. As a consequence, the ImageMagick utility could become unresponsive when converting JPEG files to PDF (Portable Document Format) files. A patch has been applied to address the deadlock issue, and JPEG files can now be properly converted to PDF files.

BZ#616538

Previously, running the "convert" command with the "-color" option failed with a memory allocation error. The source code has been modified to fix problems with memory allocation. Now, using the "convert" command with the "-color" option works correctly.

BZ#693989

Previously, ImageMagick could become unresponsive when using the "display" command on damaged GIF files. The source code has been revised to prevent the issue. ImageMagick now produces an error message in the described scenario. A file selector is now opened so the user can choose another image to display.

BZ#694922

Prior to this update, the "convert" command did not handle rotated PDF files correctly. As a consequence, the output was rendered as a portrait with the content being cropped. With this update, the PDF render geometry is modified, and the output produced by the "convert" command is properly rendered as a landscape.

All users of ImageMagick are advised to upgrade to these updated packages, which contain backported patches to correct these issues. All running instances of ImageMagick must be restarted for this update to take effect.

4.70. initscripts

4.70.1. RHSA-2012:0312 — Low: initscripts security and bug fix update

An updated initscripts package that fixes one security issue and four bugs is now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The initscripts package contains system scripts to boot your system, change runlevels, activate and deactivate most network interfaces, and shut the system down cleanly.

Security Fix

CVE-2008-1198

With the default IPsec (Internet Protocol Security) ifup script configuration, the racoon IKE key management daemon used aggressive IKE mode instead of main IKE mode. This resulted in the preshared key (PSK) hash being sent unencrypted, which could make it easier for an attacker able to sniff network traffic to obtain the plain text PSK from a transmitted hash.

Red Hat would like to thank Aleksander Adamowski for reporting this issue.

Bug Fixes

BZ#568896

Prior to this update, the DHCPv6 client was not terminated when the network service was stopped. This update modifies the source so that the client is now terminated when stopping the network service.

BZ#679998

Prior to this update, on some systems the rm command failed and reported the error message "rm: cannot remove directory `/var/run/dovecot/login/': Is a directory" during system boot. This update modifies the source so that this error message no longer appears.

BZ#744734

Prior to this update, the netconsole script could not discover and resolve the MAC address of the router specified in the /etc/sysconfig/netconsole file. This update modifies the netconsole script so that the script no longer fails when the arping tool returns the MAC address of the router more than once.

BZ#745681

Prior to this update, the arp_ip_target was, due to a logic error, not correctly removed via sysfs. As a consequence, the error "ifdown-eth: line 64: echo: write error: Invalid argument" was reported when attempting to shut down a bonding device. This update modifies the script so that the error no longer appears and arp_ip_target is now correctly removed.

All users of initscripts are advised to upgrade to this updated package, which fixes these issues.

4.71. ipa-client

4.71.1. RHBA-2011:1841 — ipa-client bug fix update

An updated ipa-client package that fixes one bug is now available for Red Hat Enterprise Linux 5.

[Updated 20 December 2011] This advisory has been updated with the correct product name (that is, Red Hat Enterprise Linux 5) in the Details section. The package included in this revised update has not been changed in any way from the package included in the original advisory.

The ipa-client package provides a tool to enroll a machine to an IPA version 2 server. IPA (Identity, Policy and Audit) is an integrated solution to provide centrally managed identity, that is, machine, user, virtual machines, groups, and authentication credentials.

Bug Fix

BZ#768058

The RHSA-2011-1533 security advisory, which fixed a security vulnerability in the IPA web-based service, caused incompatibility with older versions of ipa-client. As a consequence, ipa-client was unable to correctly submit enrollment requests to IPA. With this update, ipa-client has been modified and it now operates correctly with newer versions of IPA. Interoperability with older versions of IPA remains unaffected.

All users of ipa-client are advised to upgrade to this updated package, which fixes this bug.

4.71.2. RHBA-2011:1290 — ipa-client bug fix update

An updated ipa-client package that fixes one bug is now available for Red Hat Enterprise Linux 5.

IPA (Identity, Policy, Audit) is an integrated solution to provide centrally managed identity, that is, machine, user, virtual machines, groups, and authentication credentials. The ipa-client package provides a tool to enroll a machine to an IPA version 2 server.

Bug Fix

BZ#736658

Prior to this update, GSSAPI credential delegation was disabled in the curl utility due to a security issue. As a result, applications that rely on delegation did not work properly. This update utilizes a new constructor argument in the xmlrpc-c client API to set the new CURLOPT_GSSAPI_DELEGATION curl option. This option enables the credential delegation, thus fixing this bug.

Users of ipa-client are advised to upgrade to this updated package, which fixes this bug.

4.71.3. RHBA-2012:0190 — ipa-client bug fix update

An updated ipa-client package that fixes various bugs and adds several enhancements is now available for Red Hat Enterprise Linux 5.

The ipa-client package provides a tool to enroll a machine to an IPA version 2 server. IPA (Identity, Policy, Audit) is an integrated solution to provide centrally managed identity, that is, machine, user, virtual machines, groups, and authentication credentials.

The ipa-client package has been upgraded to upstream version 2.1.3, which provides a number of bug

fixes and enhancements over the previous version. (BZ#753936)

Bug Fixes

BZ#723667

Prior to this update, GSSAPI credential delegation was disabled in the curl utility due to a security issue. As a result, applications that rely on the delegation did not work properly. This update utilizes a new constructor argument in the xmlrpc-c client API to set the new CURLOPT_GSSAPI_DELEGATION curl option. This option enables credential delegation.

BZ#752226

A previous change to the Referer server required that a caller to the IPA server API include the Referer header in its request. Previously, requests from the certmonger and ipa administrative tools did not provide the header, and the tool requests could fail with the error "Missing or invalid HTTP Referer". However, the requests are transferred using curl and curl does not allow setting of arbitrary headers. To resolve this problem, the code has been changed so that the curl version is stored in the HTTP request field X-Original-User-Agent and the rest of the header is overridden. As a result, the correct header is used for the requests and the problem no longer occurs.

BZ#739068

If the user ran the ipa-client-install command with the password defined (for example, "ipa-client-install --principal=admin --password=SecretPsswd"), the /var/log/ipaclient-install.log file contained the password in plain text. With this update, the underlying code is modified and the provided password is no longer saved in the logs in this scenario.

BZ#710143

Previously, KDC (Key Distribution Center) autodiscovery failed if the domain name differed from the Kerberos realm name. This happened because the ipa-client-install utility always assumed that the realm name was identical to the domain name. Now the realm is used when performing autodiscovery and the problem no longer occurs.

BZ#750338

The cyrus-sasl-gssapi package is a soft dependency needed by some IPA client tools. Previously, the ipa-client package spec file did not contain the cyrus-sasl-gssapi dependency for some architectures. As a result, installation on some platforms could fail. This update adds the missing dependency to the spec file and the installation process finishes successfully.

BZ#723620

The cyrus-sasl-gssapi package is a soft dependency needed by some IPA client tools. Previously, when installing 32-bit packages on a 64-bit system, the macro determining the required architecture version of the cyrus-sasl-gssapi package did not work correctly. As a result, an incorrect version of cyrus-sasl-gssapi was installed and the system failed to work; for example, the ipa-getkeytab command failed with the following error because the 32-bit GSSAPI SASL mechanism was not available:

SASL Bind failed. This update corrects the macro and the problem no longer occurs.

All ipa-client users are advised to upgrade to this updated package, which fixes these bugs and adds

these enhancements.

4.72. iproute

4.72.1. RHBA-2011:1453 — iproute bug fix update

An updated iproute package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The iproute package contains networking utilities (ip and rtmon, for example) which are designed to use the advanced networking capabilities of the Linux kernel.

Bug Fixes

BZ#645260

Prior to this update, the ARP daemon, "arpd", had several undocumented options, including, "-?", "-B", "-R", "-b", "-h", "-k", and "-l". Consequently users issuing the command "arp --help" to see the usage message, or consulting the man page, did not see an explanation for all the options. With this update the help function's usage message and the man page have been corrected.

BZ#645264

Prior to this update, the "lnstat" usage message and man page contained spelling mistakes for the "-dump" and "-key" options. With this update these errors have been corrected.

BZ#645267

Prior to this update, the "ss" usage message and man page erroneously included an unsupported option ("-query") and omitted three supported options ("-diag", "-D", and "-socket"). With this update these errors and omissions have been corrected.

BZ#727059

Prior to this update, the "ss -4n" command did not distinguish between the "inet" and "inet6" domain when loading the tcp_diag module. Consequently IPv6 information was output in addition to the expected IPv4 information. With this update the code has been corrected and the command functions as expected.

All users of iproute are advised to upgrade to this updated package, which fixes these bugs.

4.73. iprutils

4.73.1. RHEA-2012:0185 — iprutils enhancement update

An enhanced iprutils package is now available for Red Hat Enterprise Linux 5.

The iprutils package provides utilities to manage and configure SCSI devices that are supported by the ipr SCSI storage device driver.

Enhancement

BZ#714257, BZ#760336, BZ#768532

The iprutils package has been updated to provide support for the Serial Attached SCSI (SAS)

vRAID functions.

Users of iprutils are advised to upgrade to this updated package, which adds this enhancement.

4.74. iptables

4.74.1. RHBA-2012:0255 — iptables bug fix and enhancement update

Updated iptables packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 5.

The iptables utility controls the network packet filtering code in the Linux kernel.

Bug Fixes

BZ#520797

Prior to this update, the memory alignment of ipt_connlimit_data was incorrect on x86-based systems. An error message in the format "ip_tables: connlimit match: invalid size" was logged. This update adds an explicit alignment attribute to the ipt_connlimit_data structure to correct this.

BZ#552522

The sysctl values for netfilter kernel modules were not restored after a firewall restart. Consequently, the firewall did not always perform as expected after a restart. This update applies a patch to optionally load sysctl settings on iptables start, if specified by the user in the /etc/sysctl.conf file. Users can now define sysctl settings to load on start and restart.

BZ#554340

Prior to this update, the kernel netfilter modules were not loaded at all times. Consequently, some commands did not perform as expected the first time they were executed. With this update, a patch has been applied to ensure the modules are properly loaded and the problem no longer occurs.

Enhancements

BZ#471163

Prior to this update, the statistic match module was not included in the iptables package. With this update, this module in now included.

BZ#710050

A service reload option has been added to enable a refresh of the firewall rules without unloading netfilter kernel modules and dropping connections.

Users are advised to upgrade to these updated iptables packages, which fix these bugs and add these enhancements.

4.75. iscsi-initiator-utils

4.75.1. RHBA-2012:0263 — iscsi-initiator-utils bug fix and enhancement update

An updated iscsi-initiator-utils package that fixes three bugs and adds two enhancements is now available Red Hat Enterprise Linux 5.

The iscsi-initiator-utils package provides the server daemon for the iSCSI protocol, as well as the utility programs used to manage it. iSCSI is a protocol for distributed disk access using SCSI commands sent over Internet Protocol (IP) networks.

Bug Fixes

BZ#714744

Prior to this update, the iscsiadm help wrongly listed discovery2 mode instead of discoverydb. This update modifies the help file and now the correct output of the help contents is shown.

BZ#716323

Prior to this update, iscsiadm did not accept host names or aliases as valid values for the --portal argument. As a consequence,the iscsiadm failed with the error message "iscsiadm: no records found!". This update matches the host name to the IP address returned during discovery, so this issue no longer occurs.

BZ#729355

Prior to this update, the brcm_iscsiuio daemon did not rotate the brcm-iscsi.log file. As a consequence, the log file could grow excessively. This update adds a logrotate entry for the brcm-iscsi.log file.

BZ#759651

Prior to this update,the iface net configuration parameters were not parsed on. As a consequence, the iface parameters could not be updated. This update modifies the idbm_recinfo_node routine to include the parsing of these parameters.

Enhancements

BZ#715396

This update upgrades uIP (micro IP) to the latest upstream version 0.7.0.6+ to make uIP compatible with the updated bnx2x driver.

BZ#723715

This update adds leading-login support to reduce login storms during boot and allows for initiating multiple iSCSI sessions from a single iface record.

All users of iscsi-initiator-utils are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.76. java-1.6.0-openjdk

4.76.1. RHSA-2011:1380 — Critical: java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

Security Fixes

CVE-2011-3556

A flaw was found in the Java RMI (Remote Method Invocation) registry implementation. A remote RMI client could use this flaw to execute arbitrary code on the RMI server running the registry.

CVE-2011-3557

A flaw was found in the Java RMI registry implementation. A remote RMI client could use this flaw to execute code on the RMI server with unrestricted privileges.

CVE-2011-3521

A flaw was found in the IIOP (Internet Inter-Orb Protocol) deserialization code. An untrusted Java application or applet running in a sandbox could use this flaw to bypass sandbox restrictions by deserializing specially-crafted input.

CVE-2011-3544

It was found that the Java ScriptingEngine did not properly restrict the privileges of sandboxed applications. An untrusted Java application or applet running in a sandbox could use this flaw to bypass sandbox restrictions.

CVE-2011-3548

A flaw was found in the AWT KeyStroke implementation. An untrusted Java application or applet running in a sandbox could use this flaw to bypass sandbox restrictions.

CVE-2011-3551

An integer overflow flaw, leading to a heap-based buffer overflow, was found in the Java2D code used to perform transformations of graphic shapes and images. An untrusted Java application or applet running in a sandbox could use this flaw to bypass sandbox restrictions.

CVE-2011-3554

An insufficient error checking flaw was found in the unpacker for JAR files in pack200 format. A specially-crafted JAR file could use this flaw to crash the Java Virtual Machine (JVM) or, possibly, execute arbitrary code with JVM privileges.

CVE-2011-3560

It was found that HttpsURLConnection did not perform SecurityManager checks in the setSSLSocketFactory method. An untrusted Java application or applet running in a sandbox

could use this flaw to bypass connection restrictions defined in the policy.

CVE-2011-3389

A flaw was found in the way the SSL 3 and TLS 1.0 protocols used block ciphers in cipher-block chaining (CBC) mode. An attacker able to perform a chosen plain text attack against a connection mixing trusted and untrusted data could use this flaw to recover portions of the trusted data sent over the connection.

Note

This update mitigates the CVE-2011-3389 issue by splitting the first application data record byte to a separate SSL/TLS protocol record. This mitigation may cause compatibility issues with some SSL/TLS implementations and can be disabled using the jsse.enableCBCProtection boolean property. This can be done on the command line by appending the flag "-Djsse.enableCBCProtection=false" to the java command.

CVE-2011-3547

An information leak flaw was found in the InputStream.skip implementation. An untrusted Java application or applet could possibly use this flaw to obtain bytes skipped by other threads.

CVE-2011-3558

A flaw was found in the Java HotSpot virtual machine. An untrusted Java application or applet could use this flaw to disclose portions of the VM memory, or cause it to crash.

CVE-2011-3553

The Java API for XML Web Services (JAX-WS) implementation in OpenJDK was configured to include the stack trace in error messages sent to clients. A remote client could possibly use this flaw to obtain sensitive information.

CVE-2011-3552

It was found that Java applications running with SecurityManager restrictions were allowed to use too many UDP sockets by default. If multiple instances of a malicious application were started at the same time, they could exhaust all available UDP sockets on the system.

This erratum also upgrades the OpenJDK package to IcedTea6 1.9.10. Refer to the NEWS file for further information:

http://icedtea.classpath.org/hg/release/icedtea6-1.9/file/328afd896e3e/NEWS

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

4.76.2. RHBA-2012:0314 — java-1.6.0-openjdk bug fix and enhancement update

Updated java-1.6.0-openjdk packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The java-1.6.0-openjdk packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK

6 Software Development Kit.

The java-1.6.0-openjdk packages have been upgraded to upstream version 1.2.3, which provides a number of bug fixes and enhancements over the previous version. In addition, HugePage support is now provided and can be activated with the -XX:+UseLargePages flag. (BZ#123456)

Bug Fix

BZ#751730

This update fixes a regression that caused an extra argument (-J-Djava.rmi.server.codebase) to rmiregistry to become mandatory.

Enhancements

BZ#567404

This update adds support for the Rhino JavaScript interpreter to the java-1.6.0-openjdk package.

BZ#727598

This update upgrades IcedTea6 to upstream version 1.10.

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.77. kdelibs

4.77.1. RHSA-2011:1385 — Moderate: kdelibs and kdelibs3 security update

Updated kdelibs packages for Red Hat Enterprise Linux 4 and 5 and updated kdelibs3 packages for Red Hat Enterprise Linux 6 that fix one security issue are now available.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The kdelibs and kdelibs3 packages provide libraries for the K Desktop Environment (KDE).

Security Fix

CVE-2011-3365

An input sanitization flaw was found in the KSSL (KDE SSL Wrapper) API. An attacker could supply a specially-crafted SSL certificate (for example, via a web page) to an application using KSSL, such as the Konqueror web browser, causing misleading information to be presented to the user, possibly tricking them into accepting the certificate as valid.

Users should upgrade to these updated packages, which contain a backported patch to correct this issue. The desktop must be restarted (log out, then log back in) for this update to take effect.

4.78. kernel

4.78.1. RHSA-2012:1445 — Moderate: kernel security and bug fix update

Updated *kernel* packages that fix one security issue and several bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

The *kernel* packages contain the Linux kernel, the core of any Linux operating system.

Security Fix

CVE-2012-2100, Low

It was found that the RHSA-2010:0178 update did not correctly fix the CVE-2009-4307 issue, a divide-by-zero flaw in the ext4 file system code. A local, unprivileged user with the ability to mount an ext4 file system could use this flaw to cause a denial of service.

Bug Fixes

BZ#847404

The mlx4 driver did not contain the necessary callbacks to implement Enhanced I/O Error Handling and recovery, so the PCI layer used the probe and remove callbacks to try to recover the device after an error occurred on the bus. However, a race condition occurred between these callbacks and the internal catastrophic error recovery functions which also detected the error, and consequently caused a kernel oops if both EEH and the internal recovery functions attempted to reset the device. This update adds the necessary error recovery callbacks and ensures that the internal catastrophic error functions do not try to reset the device in such scenarios. Also, additional calls have been added to suppress read and write operations on the bus when the slot cannot accept I/O operations, which prevents unnecessary accesses to the bus and speeds up the device removal.

BZ#854986

Previously, the SAS-2 tape drive was not detected after connecting it to a SATA/SAS Storage Control Unit (SCU) port. This was because the speed values in the isci driver were not updated and the negotiated connection speed for the SAS-2 device was therefore incorrect. With this update, the PHY_LINKRATE values defined in the scsi_transport_sas header file are now used, which ensures correct detection of SAS-2 devices.

BZ#856079

Previously, the code checking for a NULL pointer was incorrect; it checked for a non-NULL pointer instead. As a consequence, this could lead to a kernel panic. This update corrects the problem, so that the kernel no longer crashes in this scenario.

BZ#857552

When two processes attempted to automount an NFS file system at the same time, an account usage error occurred in the dentry of the mount point, leading to EBUSY errors when trying to unmount the file system. In addition, a kernel panic could occur when the automount timeout expired or the shutdown procedure tried to unmount the file system. This was because the vfsmount structure was missing a reference of the mount point. This update ensures that a

reference of the mount point is placed on the vfsmount structure before the do_add_mount() function is called. The NFS file system can now be unmounted as expected, and the kernel panic no longer occurs in this scenario.

BZ#857558

To resolve a kernel panic that occurred under certain circumstances, an upstream cleanup patch for VFS automount support was backported to Red Hat Enterprise Linux 5, which also fixed the panic. This upstream change occurred after the VFS automount support was added to Red Hat Enterprise Linux 5 so was not present.

BZ#857964

Prior to this update, a process of continuously opening and closing a file within a second could prevent the data cache of a file from ever expiring. This resulted in stale data being presented on the client. With this update, the modify time and size stored in cache for an existing inode are compared with the modify time and size returned by the open() call; the cache is invalidated if the values differ.

BZ#857966

A bug in the ipvs code caused insufficient performance of the Transmission Control Protocol (TCP) when generic receive offload (GRO) or generic segmentation offload (GSO) was enabled on a machine running the IP Virtual Server (IPVS) or Linux Virtual Server (LVS). The TCP connection continued to work, however, only by retransmitting all data, as only TCP segments with a single packet were allowed to go through. This update allows reception of GRO-aggregated packet buffers, through the IPVS framework. On transmission the GSO-aggregated packet buffer is automatically deaggregated by GSO. Use of GSO/GRO together with this update will result in an improved throughput and lower CPU utilization.

BZ#858774

Previously, two threads could race to automount the same Distributed File System (DFS) share. The second thread called the do_add_mount() function after the first thread had completed the automount, and received a reference to the existing vfs_mount inserted by the first thread. Consequently, the new vfs_mount created by this thread for the mount process was dropped. This resulted in the use count for the dentry pointed to by vfs_mount to drop to -1 and the system terminated with a kernel panic. The underlying source code has been modified, and a kernel panic no longer occurs under these circumstances.

BZ#859946

This update changes Xen hypervisor's behavior introduced in the CVE-2012-2934 issue: the host was prevented from booting on AMD processors with the AMD #121 erratum applied. Users were prompted to pass the "allow_unsafe" parameter on the command line to allow booting the Xen host. However, this could prevent remotely managed hosts from being started. With this update, the boot process is no longer denied by default; only guest creation is denied. The allow_unsafe semantics has changed to allow creation of guests instead of allowing booting the host.

BZ#861387

Previously, when listing of IPv6 routing table was prematurely ended, it could cause corruption of that table, leading to various problems, including a kernel panic. To prevent the problems, the routing table is now traversed correctly.

BZ#864823

A kernel panic occurred when the size of a block device was changed and I/O was issued at the same time. This was because the direct and non-direct I/O code was written with the assumption that the block size would not change. This update introduces a new read-write lock, bd_block_size_semaphore. The lock is taken for read during I/O and for write when changing block size. As a result, block size cannot be changed while I/O is being submitted. This prevents the kernel from crashing in the described scenario.

BZ#867896

On certain platforms, the be2net driver could incorrectly indicate UE bits and stop further access to be2net-based network interface cards (NICs). With this update, these UE bits are ignored and if a real UE occurs, the corresponding hardware block will automatically go offline and stop the traffic.

All users of *kernel* should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

4.78.2. RHSA-2012:1174 — Low: kernel security and bug fix update

Updated *kernel* packages that fix one security issue and multiple bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The *kernel* packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2012-2313

A flaw was found in the way the Linux kernel's dl2k driver, used by certain D-Link Gigabit Ethernet adapters, restricted IOCTLs. A local, unprivileged user could use this flaw to issue potentially harmful IOCTLs, which could cause Ethernet adapters using the dl2k driver to malfunction (for example, losing network connectivity).

Bug Fixes

BZ#830264

If a path followed a symlink that ended with the slash ("/") character, the LOOKUP_DIRECOTRY flag could be set earlier than the last path component. This led to an ENOTDIR (Not a directory) error. The LOOKUP_DIRECTORY flag is now propagated only for the last component. For the purpose of possible automounting, the flag is not needed for intermediate path components; the LOOKUP_CONTINUE flag is set in such a case. The ENOTDIR error no longer occurs in this scenario.

BZ#832448

A race condition between a device being opened and the device being disconnected occurred in the evdev code. During this condition, the evdev structure for a device continued to be used

after it had been freed. If the memory was reallocated afterward and zeroed by the new owner, the evdev_open() function could become stuck and generate a soft lockup. This update directly uses a kref structure to implement proper reference counting, which prevents the race condition from occurring in this scenario.

BZ#833182

Certain Broadcom devices, mostly the BMC5704 controllers, failed to work due to incorrect TSO (TCP Segmentation Offload) handling in the tg3 driver. The TSO handling code has been revised so that the devices now work as expected.

BZ#835450

An insufficiently designed calculation in the CPU accelerator in the previous kernel caused an arithmetic overflow in the sched_clock() function when system uptime exceeded 208.5 days. This overflow led to a kernel panic on systems using the Time Stamp Counter (TSC) or Virtual Machine Interface (VMI) clock source. This update corrects the aforementioned calculation so that this arithmetic overflow and kernel panic can no longer occur under these circumstances.

BZ#837226

On ext4 file systems, when the fallocate() system call failed to allocate blocks due to the ENOSPC condition (no space left on device) for a file larger than 4 GB, the size of the file became corrupted and, consequently, caused file system corruption. This was due to a missing cast operator in the ext4_fallocate() function. With this update, the underlying source code has been modified to address this issue, and file system corruption no longer occurs.

BZ#838140

The function used to find a resource block (rsb) during directory recovery was searching the rsb's single linear list, which took an excessive amount of time. Consequently, recovery of Distributed Lock Manager (DLM) could take a long time. With this update, the standard hash table is used to find the rsb, which decreases the search time, and DLM recovery finishes in a reasonable time.

BZ#839196

Previously, if a command timed out to a device with a reservation conflict, the SCSI error handling marked the device as offline. This was because the RESERVATION_CONFLICT return code was treated as a fatal error when a TUR command was sent to confirm that the device was reachable and responding. Consequently, the error handling progressed to the next error routine, eventually marking the device offline. The error processing in the scsi_eh_completed_normally() function has been changed to consider RESERVATION_CONFLICT for a TUR command as success. This causes the scsi_eh_tur() call to pass successfully, and the devices are no longer set as offline.

BZ#839806

When attempting to mount a NFS share twice on the same mount point, a check in the do_add_mount() function causes an error to be returned. However, when using the "noac" option, the user was abe to mount the same share on the same mount point multiple times. This was because the "noac" option was automatically assigned the MS_SYNCHRONOUS flag in the nfs_initialise_sb() function. This flag was set after the check for already existing superblocks had been performed in the sget() fucntion, and was therefore not taken into account during the check of mount flags. This update checks for the "noac" option and assigns

the MS_SYNCHRONOUS fag before sget() is called to obtain an already existing superblock structure. As a result, it is no longer possible to mount a NFS share on the same location multiple times.

BZ#840077

Failures and errors could occur due to a NULL pointer dereference in the vm_enough_memory() function. To prevent such problems, the NULL checking has been revised.

BZ#840946

In the ext4 file system, splitting an unwritten extent while using Direct I/O could fail to mark the modified extent as dirty, resulting in multiple extents claiming to map the same block. This could lead to the kernel or fsck reporting errors due to multiply claimed blocks being detected in certain inodes. In the ext4_split_unwritten_extents() function used for Direct I/O, the buffer which contains the modified extent is now properly marked as dirty in all cases. Errors due to multiply claimed blocks in inodes should no longer occur for applications using Direct I/O.

BZ#841370

When using the Intel e1000e ethernet driver, the RXCW register's invalid bit (IV) was being set periodically due to incorrect register read logic for the 82571 Serializer-Deserializer (SERDES), which resulted in link flapping. The read logic has been improved: RXCW is now read twice to filter one-time false events and obtain correct values for the IV bit. Link flaps no longer occur in this scenario.

Users of *kernel* should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

4.78.3. RHSA-2012:0690 — Important: kernel security and bug fix update

Updated *kernel* packages that fix a security issue and several bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

Security Fixes

CVE-2012-2136, Important

It was found that the ***data_len*** parameter of the **sock_alloc_send_pskb()** function in the Linux kernel's networking implementation was not validated before use. A local user with access to a TUN/TAP virtual interface could use this flaw to crash the system or, potentially, escalate their privileges. Note that unprivileged users cannot access TUN/TAP devices until the root user grants them access.

Bug Fixes

BZ#807265

When SAS (Serial Attached SCSI) disks were present on the system and the ***CK_COND=1*** parameter was set in the Command Descriptor Block (CDB), the **SAT ATA PASS-THROUGH**

commands produced a large number of irrelevant warning messages, clogging up logs with useless information. With this update, the logging has been disabled in the described scenario, thus fixing this bug.

BZ#807930

A bug in the **vsyscall** interface caused 32-bit multi-threaded programs, which received the **SIGCANCEL** signal right after they returned from a system call, to terminate unexpectedly with a segmentation fault when run on the AMD64 or Intel 64 architecture. A patch has been provided to address this issue and the crashes no longer occur in the described scenario.

BZ#809380

Previously, the restriction of the way epoll file descriptors could nest was overly aggressive. Consequently, certain applications were unable to add the desired number of epoll watches and possibly terminated unexpectedly or became unresponsive. With this update, there is no restriction on the number of epoll file descriptors that can be attached to the source file descriptor, thus preventing the described problems.

Note

Note that if an application requests a deeply-nested epoll file descriptor, the request fails gracefully rather that causing the kernel to terminate unexpectedly.

BZ#810321

Previously, secondary, tertiary, and other IP addresses added to bond interfaces could overwrite the **bond->master_ip** and **vlan_ip** values. Consequently, a wrong IP address could be occasionally used, the MII (Media Independent Interface) status of the backup slave interface went down, and the bonding master interfaces were switching. This update removes the **master_ip** and **vlan_ip** elements from the **bonding** and **vlan_entry** structures, respectively. Instead, devices are directly queried for the optimal source IP address for ARP requests, thus fixing this bug.

BZ#809791

Starting with Red Hat Enterprise Linux 5.6, all devices that used the ixgbe driver would stop stripping VLAN tags when the device entered promiscuous mode. Placing a device in a bridge group causes the device to enter promiscuous mode. This caused various issues under certain configurations of bridging and VLANs. A patch has been provided to address this issue and the devices now properly strip VLAN tags in the driver whether in promiscuous mode or not.

BZ#810123

Previously, requests for large data blocks with the **ZSECSENDCPRB** **ioctl()** system call failed due to an invalid parameter. A misleading error code was returned, concealing the real problem. With this update, the parameter for the **ZSECSENDCPRB** request code constant is validated with the correct maximum value. Now, if the parameter length is not valid, the **EINVAL** error code is returned, thus fixing this bug.

BZ#811927

When a slave started up, the active flags failed to be marked inactive while unsetting the

current_arp_slave parameter. Consequently, more than one slave with active flags in active-backup mode could be present on the system. With this update, the active flags are properly marked inactive from a slave before the ***current_arp_slave*** is unset, thus preventing this bug.

BZ#816684

When the Fibre Channel (FC) layer sets a device to "running", the layer also scans for other new devices. Previously, there was a race condition between these two operations. Consequently, for certain targets, thousands of invalid devices were created by the SCSI layer and the udev service. This update ensures that the FC layer always sets a device to "online" before scanning for others, thus fixing this bug.

Additionally, when attempting to transition priority groups on a busy FC device, the multipath layer retried immediately. If this was the only available path, a large number of retry operations was performed in a short period of time. Consequently, the logging of retry messages slowed down the system. This bug has been fixed by ensuring that the DM Multipath feature delays retry operations in the described scenario.

BZ#817691

Due to a regression, the **`ifdef`** macro was used with an invalid value. Consequently, the **`tg3`** driver did not support VLAN tagging and the **`vconfig`** utility was unable to configure VLAN tagging properly, thus blocking the network connection. This update removes incorrect usages of **`ifdef`** from the code and the VLAN support now works as expected.

Users should upgrade to these updated packages, which contain backported patches to resolve this issue and fix these bugs. The system must be rebooted for this update to take effect.

4.78.4. RHSA-2012:0480 — Important: kernel security, bug fix, and enhancement update

Updated *kernel* packages that fix several security issues and bugs, and add an enhancement are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

Security Fixes

CVE-2012-1583, Important

A flaw in the **`xfrm6_tunnel_rcv()`** function in the Linux kernel's IPv6 implementation could lead to a use-after-free or double free flaw in **`tunnel6_rcv()`**. A remote attacker could use this flaw to send specially-crafted packets to a target system that is using IPv6 and also has the **`xfrm6_tunnel`** kernel module loaded, causing it to crash.

Note

If you do not run applications that use **xfrm6_tunnel**, you can prevent the **xfrm6_tunnel** module from being loaded by creating (as the root user) a **/etc/modprobe.d/xfrm6_tunnel.conf** file, and adding the following line to it:

```
blacklist xfrm6_tunnel
```

This way, the **xfrm6_tunnel** module cannot be loaded accidentally. A reboot is not necessary for this change to take effect.

Bug Fixes

BZ#795664

In NFSv4, both write and open code paths depended on the **I_LOCK** flag in **inode->i_state**. In addition to this, the write code path also needs the latest **stateid** returned by open to before it can proceed. It waits for this while holding the **I_LOCK** bit in **inode->state**. As a consequence, multi-threaded applications could be blocked when using NFSv4. With this update, the **nfs_fhget()** function has been modified to use the **I_NEW** flag for the open code path, thus fixing this bug.

BZ#798748

Due to a bug in the **qla2xxx** driver and the HBA firmware, storage I/O traffic could become unresponsive during storage fault testing. With this update, these bugs have been fixed and the hangs no longer happen in the described scenario.

BZ#799941

When a single, large data stream was being written to an NFS server while other applications periodically wrote small amounts of data to a local file system, other applications could experience long pauses when dirty memory reaches the **dirty_ratio** limit. With this update, the code for **COMMIT** calls has been improved to not skip such calls if the system is under memory pressure and to allow high priority **COMMIT** calls to bypass inode commit locks. Now, the pauses in traffic no longer occur in the described scenario.

BZ#801724

The QDIO (Queued Direct I/O) data transfer architecture maintains a "buffers-used" counter for its hardware buffers. If the buffers were returned in the **ERROR** state, the counter was updated incorrectly when running under the **z/VM** operating system with the **QIOASSIST** flag switched on. Consequently, the buffer handling logic in QDIO was working incorrectly. This update fixes the code to update the counter correctly in the described scenario, thus fixing this bug.

BZ#801726

The **vfs-automount** infrastructure assumes that the **LOOKUP_DIRECTORY** flag is included in **nameidata** flags if a trailing slash character (**/**) is given on a path being walked. But this flag is private to the **__link_path_walk()** function so it must be added when looking up the last component. Previously, during a path walk where the path included a trailing slash character,

LOOKUP_DIRECTORY was not propagated to path walk functions. Consequently, directories that needed to trigger an automount failed to do so, which resulted in a **-ENOTDIR** error. This bug has been fixed and the error code is no longer returned in the described scenario.

BZ#804721

If the IP stack proper is accessed from bridge netfilter, the socket buffer needs to be in a form the IP stack expects. Previously, the entry point on the **NF_FORWARD** hook did not meet the requirements of the IP stack. Consequently, hosts could terminate unexpectedly. A backported upstream patch has been provided to address this issue and the crashes no longer occur in the described scenario.

BZ#805460

When the **kvmclock** initialization was used in a guest, it could write to the time stamp counter (TSC) and, under certain circumstances, could cause the kernel to become unresponsive on boot. With this update, TSC synchronization, which is unnecessary due to **kvmclock**, has been disabled, thus fixing this bug.

BZ#805462

When using the **be2net** driver, if a card was reset due to EEH (Enhanced Error Handling), the error recovery involves ring clean-up and re-creation. However, because worker threads touch this ring, there was a race condition that caused kernel to terminate unexpectedly. With this update, a worker thread is stopped during this clean-up process, thus preventing this bug.

Enhancements

BZ#770649

This update adds support for mount options to restrict access to **/proc/<PID>/** directories. One of the options is called **hidepid=** and its value defines how much information about processes is provided to non-owners. The **gid=** option defines a group that gathers information about all processes. Untrusted users, which are not supposed to monitor tasks in the whole system, should not be added to the group.

Users should upgrade to these updated packages, which contain backported patches to resolve this issue, fix these bugs, and add this enhancement. The system must be rebooted for this update to take effect.

4.78.5. RHSA-2012:0150 — Moderate: Red Hat Enterprise Linux 5.8 kernel security, bug fix, and enhancement update

Updated *kernel* packages that fix one security issue, address several hundred bugs, and add numerous enhancements are now available as part of the ongoing support and maintenance of Red Hat Enterprise Linux version 5. This is the eighth regular update.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, is available from the CVE link associated with the description below.

The *kernel* packages contain the Linux kernel, the core of any Linux operating system.

Security Fix

CVE-2011-1083, Moderate

A flaw was found in the way the Linux kernel's Event Poll (epoll) subsystem handled large, nested epoll structures. A local, unprivileged user could use this flaw to cause a denial of service.

Red Hat would like to thank Nelson Elhage for reporting this issue.

Bug Fixes

BZ#782773

Prior to this update, kernel panic could occur on AMD systems with HPC mode enabled in their BIOS configuration. This BIOS option disables some of the P-states supported by the system. The powernow-k8 driver erroneously relied on the consecutive numbering of the P-states, which is not given anymore in this case. With this update, the enabled P-states are properly recognized, and kernel panic no longer occurs.

BZ#721361

Certain systems do not correctly set the ACPI FADT APIC mode bit. They set the bit to "cluster" mode instead of "physical" mode which caused these systems to boot without the TSC. With this update, the ACPI FADT check has been removed due to its unreliability, thus, fixing this issue.

BZ#720551

Under some circumstances, error reports within the XFS file system could dereference a NULL pointer causing a kernel panic. This update fixes the NULL pointer dereference, and the kernel panic no longer occurs.

BZ#772696

Transmitting a fragmented socket buffer (skb) with more than 8 fragments on architectures with pages larger than 8 KiB could cause the qlge 10 Gigabit Ethernet driver to fail to properly unmap the mapped DMA addresses in order to successfully transmit all the fragments of the skb. This update adjusts the size of the external list that is used when the number of skb fragments is greater than the size of the pages; thus, fixing this issue.

BZ#720363

Due to a regression, the byte count on the wrong buffer was adjusted to account for endian differences. This resulted in the wrong buffer length being passed to the callers on big endian machines, which in turn resulted in data returned from the server being incorrectly rejected with the following error messages.

```
Invalid transact2 SMB:
```

This bug was first reported on the 64-bit PowerPC architecture. With this update, the correct buffer length is now passed in the described scenario.

BZ#722302

Packet statistics in /proc/net/dev occasionally jumped backwards. This was because the cat /proc/net/dev command was processed while the loop updating the counter was running, sometimes resulting in partially updated counter (causing the statistics to be incorrect). This update fixes this bug by using a temporary variable while summing up all the RX queues, and only then updating the /proc/net/dev statistics, making the whole operation atomic. Additionally, this update provides a patch that fixes a problem with the 16-bit RX dropped packets HW counter by maintaining a 32-bit accumulator in the driver to prevent frequent wraparound.

BZ#720212

When kdump was triggered under a heavy load, the system became unresponsive and failed to capture a crash dump. This update fixes interrupt handling for kdump so that kdump successfully captures a crash dump while under a heavy load.

BZ#722549

This update fixes a race between TX and MCC events where an MCC event could kill a NAPI schedule by a succeeding TX event, which resulted in network transfer pauses.

BZ#585935

Previously, when the iput() function was called while it held the nfs_access_lru lock could result in problems since iput() can sleep, and it can also attempt to allocate memory. This update removes an optimization that is not present in the mainline kernel series. Now, iput() is never called while holding a spinlock in the nfs_access_cache_shrinker(), thus preventing this bug.

BZ#718232

A problem with the XFS dio error handling was discovered. If a misaligned write I/O operation was issued, XFS would return -EINVAL without unlocking the inode's mutex. This caused any further operations on the inode to become unresponsive. This update adds a missing mutex_unlock operation to the dio error path, solving this issue.

BZ#724923

An incorrect call to the nfs4_drop_state_owner function caused the NFSv4 state reclaimer thread to be stuck in an infinite loop while holding the Big Kernel Lock (BKL). With this update, the aforementioned call has been removed, thus, fixing this issue.

BZ#725573

The fix for CVE-2010-3432 provided in RHSA-2011:0004 introduced a regression: Information in sctp_packet_config(), which was called before appending data chunks to a packet, was not reset, causing considerably poor SCTP (Stream Control Transmission Protocol) performance. With this update, the packet information is reset after transmission.

BZ#725713

Previously, the inet6_sk_generic() function was using the obj_size variable to compute the address of its inner structure, causing memory corruption. With this update, the sk_alloc_size() is called every time there is a request for allocation, and memory corruption no longer occurs.

BZ#727504

A previously applied patch introduced a regression for 3rd party file systems that do not set the

FS_HAS_IODONE2 flag, specifically, the Oracle Cluster File System 2 (OCFS2). The patch removed a call to the aio_complete function, resulting in no completion events being processed, causing userspace applications to become unresponsive. This update reintroduces the aio_complete function call, fixing this issue.

BZ#727614

Previously, configurations where Max BW was set to 0 produced the following message:

```
Illegal configuration detected for Max BW - using 100 instead.
```

With this update, such message is produced only when debugging is enabled, and such configuration is no longer called Illegal.

BZ#637930

Under certain circumstances, a deadlock could occur between the khubd process of the USB stack and the modprobe of the usb-storage module. This was because the khubd process, when attempting to delete a USB device, waited for the reference count of knode_bus to be of value 0. However, modprobe, when loading the usb-storage module, scans all USB devices and increments the reference count, preventing the khubd process from continuing. With this update, the underlying source code has been modified to address this issue, and a deadlock no longer occurs in the described scenario.

BZ#728219

Kernel panic occurred on a Red Hat Enterprise Linux 5.7 QLogic FCoE host during I/O operations with fabric faults due to a NULL fcport object dereference in the qla24xx_queuecommand function. This update adds a check that returns DID_NO_CONNECT if the fcport object is NULL.

BZ#728508

A previously introduced patch forced the ->flush and ->fsync operations to wait on all WRITE and COMMIT remote procedure calls (RPC) to complete to ensure that those RPCs were completed before returning from fsync() or close(). As a consequence, all WRITEs issued by nfs_flush_list were serialized and caused a performance regression on NFS clients. This update changes nfs_flush_one and nfs_flush_multi to not wait for WRITEs issued when the FLUSH_SYNC parameter is set, resolving performance issues on NFS clients.

BZ#716821

Older versions of be2net cards firmware may not have recognized certain commands and returned illegal/unsupported errors, causing confusing error messages to appear in the logs. With this update, the driver handles these errors gracefully and does not log them.

BZ#657345

When a host was in recovery mode and a SCSI scan operation was initiated, the scan operation failed and provided no error output. This bug has been fixed and the SCSI layer now waits for recovery of the host to complete scan operations for devices.

BZ#730097

Prior to this update, the nosharecache NFS mount option was not always honored. If two mount

locations specified this option, the behavior would be the same as if the option was not specified. This was because of missing checks that enforced this option. This update adds the missing checks, resolving this issue.

BZ#730108

If the be2net driver could not allocate new SKBs in the RX completion handler, it returned messages to the console and dropped packets. With this update, the driver increases the netdevice rx_dropped counter instead, and no longer produces messages in the console.

BZ#730313

When the hangcheck timer expires and tries to reboot the machine, it stops all other CPUs in the configuration. However, the CPU that stops the other CPUs is still enabled for interrupts. Consequently, I/O or external interrupts might arrive at the local CPU and the corresponding interrupt handler might try to acquire a lock. Previously, if a remote CPU was holding the lock while the local CPU stopped it, the result was a deadlock. The system became unresponsive instead of performing a reboot. With this update, interrupts are disabled before stopping remote CPUs and the hangs no longer occur in the described scenario.

BZ#758923

When a network device was renamed, the IPv6 snmp6 code did not register the change and caused the system to panic on some architectures when the device was removed. With this update, un-registering and re-registering now works as expected, and kernel panic no longer occurs.

BZ#675781

When reading a file from a subdirectory in /proc/bus/pci/ while hot-unplugging a device related to that file, the system would crash. With this update, the kernel correctly handles the simultaneous removal of a device, and access to the representation of that device in the proc file system.

BZ#731599

A KVM guest can get preempted by the host, when a higher priority process needs to run. When a guest is not running for several timer interrupts in a row, ticks could be lost, resulting in the jiffies timer advancing slower than expected and timeouts taking longer than expected. To correct for the issue of lost ticks, do_timer_tsc_timekeeping() checks a reference clock source (kvm-clock when running as a KVM guest) to see if timer interrupts have been missed. If so, jiffies is incremented by the number of missed timer interrupts and ensuring that programs are woken up on time.

BZ#731806

The be2net driver does not use lock-less Tx paths and its xmit() function is protected by the netif_tx_lock spinlock; as are the set_multicast_list() and set_rx_mode() functions. This configuration setup involves sending a message to the card firmware and getting a reply back, which involves delay up to several miliseconds long. As a consequence, the requeue counter increased by high numbers. With this update, the NETIF_F_LLTX feature has been enabled and locking of own Tx paths has been implemented. Now, only small portions of multicast configuration needs to be locked in the described scenario.

BZ#680411

Prior to this update, failures to bring up the Broadcom BCM57710 Ethernet Controller occurred and the following error messages:

```
eth0: Something bad had happen! Aii!
[bnx2x_release_hw_lock:1536(eth0)]Releasing a lock on resource 8
eth0: Recovery flow hasn't been properly completed yet. Try again later. If
u
still see this message after a few retries then power cycle is required.
```

With this update, the underlying source code has been modified to address this issue, and the Broadcom BCM57710 Ethernet Controller no longer fails to start.

BZ#721173

The iscsi offload feature of the cxgb3 driver contained a driver bug in which in-process I/O operations may have attempted to access a control data structure after it was freed in response to a hardware error that disabled the offload functionality. The driver has been corrected to enforce delaying the freeing of this structure until all in-flight operations are complete.

BZ#714020

In some cases, a client skipped issuing a COMMIT call to the server when it determined that it will need to do another such call in the near future. Consequently, the NFS code failed to re-mark the inode as dirty, and the VFS file system failed to issue the call on the next pass. The inode had pages that needed to be cleaned but the inode itself was not marked as dirty. The kdump tuned writeback thresholds to a very low value in order to keep the page cache small. In this environment, the above bug often caused the client to become unresponsive when writing out the vmcore file. With this update, an upstream patch has been provided to address this issue and the hangs no longer occur.

BZ#713904

The unsolicited frame control infrastructure requires a table of DMA addresses for the hardware to look up the frame buffer location by an index. The hardware expects the elements of this table to be 64-bit quantities. Previously, the dma_addr_t parameter was wrongly used to reference these elements. Consequently, all unsolicited frame protocols were affected, particularly SATA-PIO and SMP, which prevented direct-attached SATA drives and expander-attached drives from being discovered. A patch has been provided to address this issue and SATA drives are now recognized correctly on 32-bit platforms.

BZ#756412

kexec/kdump attempts to detect spurious interrupt requests; that is, interrupts that are left in an asserted state at the time the kernel triggers the dump. In some cases, the IDE interrupt handler would not acknowledge its interrupt, so that it would be considered spurious despite being used by the kdump kernel. As a result, the kdump kernel would take a lock twice on the IDE interrupt line and the system would become unresponsive. To fix this bug, the kexec/kdump now treats an interrupt as spurious if the corresponding interrupt line is disabled. The IDE interrupt handler is not be handled specially, and the wrong recursive lock will not occur.

BZ#683393

If management firmware is present and a device is down, the firmware assumes control of the

phy register. Previously, phy access was allowed from the host and it collided with firmware phy accesses, resulting in unpredictable behavior such as BMC (Baseboard Management Controller) LAN link being lost over time. With this update, the bug is fixed in the tg3 driver by only allowing phy accesses while the driver has control of the device.

BZ#713816

When a 10 Gigabit Ethernet BladeEngine 3 (BE3) I/O controller chip was configured to support iSCSI, the installation of Red Hat Enterprise Linux 5.7 became unresponsive. When the be2net and be2iscsi drivers were both used, the be2iscsi driver did not clean up its resources properly and caused the be2net driver to fail to load. This update adds a shutdown routine to the be2iscsi driver, and the system no longer hangs in the aforementioned scenario.

BZ#734900

In certain circumstances, the evdev_pass_event() function with a spinlock attached was interrupted and called again, eventually resulting in a deadlock. A patch has been provided to address this issue by disabling interrupts when the spinlock is obtained. This prevents the deadlock from occurring.

BZ#753924

Previously, the domain_update_iommu_coherency() function set domains, by default, as coherent when the domain was not attached to any input/output memory management units (IOMMUs). Consequently, such a domain could update context entries non-coherently via the domain_context_mapping_one() function. To resolve this issue, domain_update_iommu_coherency() has been updated to use the safer default value and domains not attached to any IOMMU are now set as non-coherent.

BZ#691087

When setting the value in the /proc/sys/vm/dirty_writeback_centisecs file via echo, the actual saved value was always one less than the given value (for example, setting 500 resulted in 499 being set). This update fixes this off-by-one error, and values in /proc/sys/vm/dirty_writeback_centisecs are now correctly set.

BZ#713703

This patch fixes the inability of the be2net driver to work in a kdump environment. It clears an interrupt bit (in the card) that may be set while the driver is probed by the kdump kernel after a crash.

BZ#748999

A previous kernel patch removed a call in the nfs_file_release() function to the filemap_fdatawrite() function. Consequently, data written to a NFS file, which had been mapped into memory via the mmap() function and not yet flushed to the backing device, were lost as soon as the file was closed. This update adds the filemap_fdatawrite() call back to the nfs_file_flush() function, which fixes this regression.

BZ#692966

Changes made to TSC as a clock source for IRQs caused virtual machines running under the VMware ESX or ESXi hypervisors to become unresponsive during the initial kernel boot process. With this update, the enable_tsc_timer flag enables the do_timer_tsc_timekeeping()

function to be called in the do_timer_interrupt_hook() function, preventing a deadlock in the timer interrupt handler, and fixing this bug.

BZ#740898

Due to unbalanced page locking in the ext4 file system write and I/O submission path, a page might have been left locked in certain error situations, eventually causing a deadlock. This was fixed by properly unlocking the page in given situations so that the deadlock no longer occur.

BZ#696430

Under a high load, a user-space application did not receive data out of the SCTP SEQ_PACKET socket. When buffer space or memory allocations failed, data chunks were dropped. However, the TSN (Transmission Sequence Number) was still reported to be successfully received, resulting in data loss. With this update, the SCTP stack has been fixed to properly report chunks that have been dropped due to memory allocation failures.

BZ#710272

If iSCSI was not supported on a bnx2 device, the bnx2_cnic_probe() function returned NULL and the cnic device was not be visible to bnx2i. This prevented bnx2i from registering and then unregistering during cnic_start() and caused the following warning message to appear:

```
bnx2 0003:01:00.1: eth1: Failed waiting for ULP up call to complete
```

BZ#698728

Prior to this update, the ndisc_send_skb() function was using an incorrect macro to increment the ICMP6 statistics. As a result, an out-of-bound element in an array which resides in the size-128 slab pool was incremented, causing data corruption. If the array was near the end of the slab page, user data corruption could occur. This update fixes the above-mentioned function to use the correct macro for incrementing the ICMP6 statistics, and data corruption no longer occurs.

BZ#742514

Previously, link power down could not be used. The code for it was already in place but was disabled. With this update, link power down has been enabled in the code and works as expected.

BZ#751214

A previous patch introduced with BZ#732775 had the following unintended consequence: if no poll method was defined for files in the /proc/ directory, processes could become unresponsive while they were reading files from this directory. This update restores the default poll behavior for files in /proc/ that do not have any poll method defined, thus fixing this bug.

Note

Note that procfs files are not real files and unless they may specifically produce more data after a time (such as /proc/kmsg), they should not be polled for more data as some of them cannot be polled for reading. For the most part, all the data they can produce are instantly available.

BZ#707425

When a block device object was allocated, the bd_super field was not being explicitly initialized to NULL. Previous users of the block device object may have set the bd_super field to NULL when the object is released by calling the kill_block_super() function. Some third party file systems do not always use this function and as a result the bd_super field could have become uninitialized when the object was allocated again. This could cause a kernel panic in the blkdev_releasepage() function when the uninitialized bd_super field was dereferenced. With this update, the bd_super field is properly initialized in the bdget function, and kernel panic no longer occurs.

BZ#746272

On a system with an idle network interface card (NIC) controlled by the e1000e driver, when the card transmitted up to four descriptors, which delayed the write-back and nothing else, the run of the watchdog driver about two seconds later forced a check for a transmit hang in the hardware, which found the old entry in the TX ring. Consequently, a false "Detected Hardware Unit Hang" message was issued to the log. With this update, when the hang is detected, the descriptor is flushed and the hang check is run again, which fixes this bug.

BZ#700886

With this update, IBM System x3850 X5 is now properly identified as a multi-chassis system by querying the system name and checking for multiple Chassis entries in the SMBIOS table. If multiple Chassis entries are found, the TSC is marked as unsynchronized. The side effect of this solution is that the kernel will attempt to synchronize the TSC on every CPU during system boot which will cause a small delay and error message to be displayed. For other multi-chassis systems, the "notsc" boot parameter can be used to disable the TSC.

BZ#748792

Incorrect duplicate MAC addresses were being used on a rack network daughter card that contained a quad-port Intel I350 Gigabit Ethernet Controller. With this update, the underlying source code has been modified to address this issue, and correct MAC addresses are now used under all circumstances.

BZ#704192

Prior to this update, a race condition in TIPC's (Transparent Inter-process Communication) recv_msg function caused kernel panic. This update modifies TIPC's socket locking logic, and kernel panic no longer occurs.

BZ#701574

The RHSA-2009:1243 update introduced a regression in the way file locking on NFS (Network File System) was handled. This caused applications to hang if they made a lock request on a file on an NFS version 2 or 3 file system that was mounted with the "sec=krb5" option. With this update, the original behavior of using mixed RPC authentication flavors for NFS and locking requests has been restored.

BZ#709699

Previously, if a connect change occurs on a USB device, it is reported the same way as a disconnect. As a consequence, the "hub 1-1.6:1.0: Cannot enable port X. Maybe the USB cable

is bad?" were issued by the dmesg utility when a low speed USB device was connected to port X. With this update, the port reset code in the hub driver has been changed, code of the usb_reset_device() function has been fixed to prevent the routine from futilely retrying the reset after a disconnect has occurred, and no error messages are now returned in the described scenario.

BZ#742079

When the SMP (Symmetric Multi Processing) kernel ran the crash_kexec() function, the local Advanced Programmable Interrupt Controllers (APICs) could have pending interrupt requests (IRQs) in their vector tables. If there was more than one pending IRQ within the same 32-bit word in the Local APIC (LAPIC) vector table registers, the I/O APIC subsystem would enter setup with pending interrupts left in the LAPIC, causing various degrees of malfunctioning depending on the stuck interrupt vector. This update adds the MAX_LOOPS parameter to limit number of iterations and to provide enough time for the pending IRQs to be cleared if the loop was to lock-up for whatever reason, thus fixing this bug.

BZ#694625

In error recovery, most SCSI error recovery stages send a TUR (Test Unit Ready) command for every bad command when a driver error handler reports success. When several bad commands pointed to a same device, the device was probed multiple times. When the device was in a state where it did not respond to commands even after a recovery function returned success, the error handler had to wait for the commands to time out. This significantly impeded the recovery process. With this update, SCSI mid-layer error routines to send test commands have been fixed to respond once per device instead of once per bad command, thus reducing error recovery time considerably.

BZ#739665

Previously, kernel was allowed to reduce the number of unnecessary commit calls by skipping the commit when there was a large number of outstanding pages being written. However, that test did not properly handle the edge case when the number of commits (ncommit) was zero. Consequently, inodes sometimes remained on the sb->s_dirty list and could not be freed by the inode cache shrinker. As a result, the nfs_inode_cache structure grew very large over time. With this update, the call to the nfs_write_inode() function is immediately returned when commit == 0, thus fixing this bug.

BZ#636828

When a COOKIE_ACK message with a packet length smaller then the chunk length defined was received, SCTP (Stream Control Transmission Protocol) sent an ABORT message with incorrectly encoded PROTOCOL VIOLATION error cause. With this update, the underlying code has been fixed and the ABORT message is now encoded properly in the described scenario.

BZ#635982

The operational state of a network device, represented by the value in /sys/class/net/eth<X>/operstate, was not initialized by default and reported unknown when the network device was up and was using the tg3 driver. This update fixes the tg3 driver to properly set the operstate value.

BZ#629938

When an INIT_ACK packet is sent with no STATE COOKIE mandatory parameter, the expected

abort error cause is Mandatory Parameter missing. Previously, the Invalid mandatory parameter error cause was given instead. With this update, a bug in the sctp_process_missing_param() function has been fixed and now, correct error cause value for missing parameters is set in the described scenario.

BZ#771592

SG_IO ioctls were not implemented correctly in the Red Hat Enterprise Linux 5 virtio-blk driver. Sending an SG_IO ioctl request to a virtio-blk disk caused the sending thread to enter an uninterruptible sleep state ("D" state). With this update, SG_IO ioctls are rejected by the virtio-blk driver: the ioctl system call will simply return an ENOTTY ("Inappropriate ioctl for device") error and the thread will continue normally.

BZ#717959

When directories mounted on a server are rearranged, they may then nest in a different order and clients may become unable to see or reassign the directories properly. Previously, the __d_unalias() and __d_materialise_dentry() functions did not provide loop prevention. As a consequence, NFS threads sometimes became unresponsive upon encountering a loop in the dentry tree. To fix this bug, this update adds additional loop checks and if a process tries to access a dentry that would otherwise cause the kernel to complete the loop, the ELOOP error code is returned and a message is logged.

BZ#719495

Prior to this update, an attempt to use the vfree() function on a vmalloc()'ed area could result in a memory leak. With this update, the underlying source code has been modified to address this issue, and a memory leak no longer occurs.

BZ#722482

On IBM System z, if a Linux instance with large amounts of anonymous memory runs into a memory shortage the first time, all pages on the active or inactive lists are considered referenced. This causes the memory management on IBM System z to do a full check over all page cache pages and start writeback for all of them. As a consequence, the system became temporarily unresponsive when the described situation occurred. With this update, only pages with active mappers are checked and the page scan now does not cause the hangs.

BZ#718988

This update adds a missing patch that enables WOL (Wake-on-LAN) on the second port of a Intel Ethernet Server Adapter I350.

BZ#730247

A previously introduced patch reduced the size of the DMA zone under the Xen hypervisor. Consequently, drivers trying to allocate contiguous memory with the dma_alloc_coherent() API often had their requests fail. This resulted in BIOS update failures on some systems with large flash memory. With this update, the zone restriction in dma_alloc_coherent() is relaxed, thus fixing this issue.

BZ#707966

A previously applied patch to help clean-up a failed nmi_watchdog check by disabling various registers caused single-vcpu Xen HVM guests to become unresponsive during boot when the

host CPU was an Intel Xeon Processor E5405 or an Intel Xeon Processor E5420, and the VM configuration did not have the apic = 1 parameter set. With this update, NMI_NONE is the default watchdog on AMD64 HVM guests, thus, fixing this issue.

BZ#740203

A previously applied patch (introduced as a fix in CVE-2011-1898) prevented PCI pass-through inside the assign_device domctl via a security check. Because the security check was not included in the test_assign_device domctl as well, qemu-dm may have started to encounter failures in the assign_device domctl, ultimately causing an HVM guest to have a partly accessible PCI device, which in some cases resulted in a crash of the host machine. With this update, the security check introduced in CVE-2011-1898 has been replicated in the test_assign_device domctl, thus fixing this issue.

BZ#723755

Prior to this update, Xen did not implement certain ALU opcodes. As a result, when a driver used the missing opcodes on memory-mapped I/O areas, it caused the guest to crash. This update adds all the missing opcodes. In particular, this fixes a BSOD crash from the Windows e1000 driver.

BZ#700565

A bug was found in the way the x86_emulate() function handled the IMUL instruction in the Xen hypervisor. On systems that have no support for hardware assisted paging (such as those running CPUs that do not have support for Intel Extended Page Tables or AMD Rapid Virtualization Indexing), or have it disabled, this bug could cause fully-virtualized guests to crash or lead to silent memory corruption. In reported cases, this issue occurred when booting fully-virtualized Red Hat Enterprise Linux 6.1 guests with memory cgroups enabled.

BZ#729529

Previously, when the Xen hypervisor split a 2 MB page into 4 KB pages, it linked the new page from the PDE (Page Directory Entry) before it filled entries of the page with appropriate data. Consequently, when doing a live migration with EPT (Extended Page Tables) enabled on a non-idle guest running with more than two virtual CPUs, the guest often terminated unexpectedly. With this update, the Xen hypervisor prepares the page table entry first, and then links it in, fixing this bug.

BZ#746225

The Xen network back-end driver was supposed to turn on all of its possible features until it negotiated with the front-end. However, after the negotiation, it did not disable the features declined by the front-end. This caused Windows guest using the xenpv-win network driver to not be able to transmit data to the host over TCP. This update properly disables the features which are not supported by the front-end.

BZ#697021

Prior to this update, MTU was constrained to 1500 unless Scatter/Gather I/O (SG) was supported by the NIC; in the case of netback, this would mean unless SG was supported by the front-end. Because the hotplugging scripts ran before features have been negotiated with the front-end, at that point SG would still be disabled, breaking anything using larger MTUs, (for example, cluster communication using that NIC). This update inverts the behavior and assumes SG to be present until negotiations prove otherwise (in such a case, MTU is automatically

reduced).

Enhancements

The *Red Hat Enterprise Linux 5.8 Release Notes* list the most important changes in the *kernel* package introduced with this update, specifically: Chapter 3. Device Drivers contains a list of updated kernel device drivers, and Chapter 2. Kernel includes major kernel enhancements.

BZ#715603

This update makes the size of the three DLM hash tables consistent: 1024 entries with a Red Hat Enterprise Linux 5-specific change to allocate the tables using vmalloc allowing a higher maximum size that can be allocated for these tables. This results in improved DLM/GFS performance when there are many locks being held (that is, many GFS files being used).

BZ#738440

This update improves the performance of delete/unlink operations in a GFS2 file system containing large files by adding a layer of metadata read-ahead for indirect blocks.

BZ#707051

With this update, the JSM driver has been updated to support the Bell2 (with PLX chip) 2-port adapter on IBM POWER7 systems. Additionally, EEH support has been added to JSM driver.

BZ#765751

Starting with Red Hat Enterprise Linux 5.8, the size of IO operations allowed by the NFS server has been increased by default. The new default max block size varies depending on RAM size, with a maximum of 1M (1048576 bytes).

Important

This may cause problems for 32-bit servers configured to use large numbers of nfsd threads. For such servers, we recommend decreasing the number of threads, or decreasing the IO size by writing to /proc/fs/nfsd/max_block_size before starting nfsd. For example, "echo 32767 >/proc/fs/nfsd/max_block_size" will restore the previous default iosize of 32k.

BZ#733416

This update introduces support for jumbo frames in the Xen networking backend. However, old guests will still revert to a 1500-byte MTU after migration. This update also changes how the guest will probe the backend's Scatter/Gather I/O functionality. As long as a recent enough kernel is installed in the destination host, this will ensure that the guest will keep a large MTU even after migration.

All Red Hat Enterprise Linux 5 users are advised to install these updated packages, which correct these issues and add these enhancements. The system must be rebooted for this update to take effect.

4.78.6. RHSA-2012:0107 — Important: kernel security and bug fix update

Updated kernel packages that fix multiple security issues and two bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2011-4127, Important

Using the SG_IO ioctl to issue SCSI requests to partitions or LVM volumes resulted in the requests being passed to the underlying block device. If a privileged user only had access to a single partition or LVM volume, they could use this flaw to bypass those restrictions and gain read and write access (and be able to issue other SCSI commands) to the entire block device. Refer to Red Hat Knowledgebase article DOC-67874, linked to in the References, for further details about this issue.

CVE-2012-0028, Important

A flaw was found in the way the Linux kernel handled robust list pointers of user-space held futexes across exec() calls. A local, unprivileged user could use this flaw to cause a denial of service or, eventually, escalate their privileges.

CVE-2011-3638, Moderate

A flaw was found in the Linux kernel in the way splitting two extents in ext4_ext_convert_to_initialized() worked. A local, unprivileged user with the ability to mount and unmount ext4 file systems could use this flaw to cause a denial of service.

CVE-2011-4086, Moderate

A flaw was found in the way the Linux kernel's journal_unmap_buffer() function handled buffer head states. On systems that have an ext4 file system with a journal mounted, a local, unprivileged user could use this flaw to cause a denial of service.

CVE-2012-0207, Moderate

A divide-by-zero flaw was found in the Linux kernel's igmp_heard_query() function. An attacker able to send certain IGMP (Internet Group Management Protocol) packets to a target system could use this flaw to cause a denial of service.

Red Hat would like to thank Zheng Liu for reporting CVE-2011-3638, and Simon McVittie for reporting CVE-2012-0207.

Bug Fixes

BZ#772162

When a host was in recovery mode and a SCSI scan operation was initiated, the scan operation failed and provided no error output. This bug has been fixed and the SCSI layer now waits for recovery of the host to complete scan operations for devices.

BZ#773322

SG_IO ioctls were not implemented correctly in the Red Hat Enterprise Linux 5 virtio-blk driver. Sending an SG_IO ioctl request to a virtio-blk disk caused the sending thread to enter an uninterruptible sleep state ("D" state). With this update, SG_IO ioctls are rejected by the virtio-blk driver: the ioctl system call will simply return an ENOTTY ("Inappropriate ioctl for device") error and the thread will continue normally.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

4.78.7. RHSA-2012:0007 — Important: kernel security, bug fix, and enhancement update

Updated kernel packages that fix multiple security issues, several bugs, and add one enhancement are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2011-4077, Important

A buffer overflow flaw was found in the way the Linux kernel's XFS file system implementation handled links with overly long path names. A local, unprivileged user could use this flaw to cause a denial of service or escalate their privileges by mounting a specially-crafted disk.

CVE-2011-4348, Important

The fix for CVE-2011-2482 provided by RHSA-2011:1212 introduced a regression: on systems that do not have Security-Enhanced Linux (SELinux) in Enforcing mode, a socket lock race could occur between sctp_rcv() and sctp_accept(). A remote attacker could use this flaw to cause a denial of service. By default, SELinux runs in Enforcing mode on Red Hat Enterprise Linux 5.

CVE-2011-1020, Moderate

The proc file system could allow a local, unprivileged user to obtain sensitive information or possibly cause integrity issues.

CVE-2011-3637, Moderate

A missing validation flaw was found in the Linux kernel's m_stop() implementation. A local, unprivileged user could use this flaw to trigger a denial of service.

CVE-2011-4132, Moderate

A flaw was found in the Linux kernel's Journaling Block Device (JBD). A local attacker could use this flaw to crash the system by mounting a specially-crafted ext3 or ext4 disk.

CVE-2011-4324, Moderate

A flaw was found in the Linux kernel's encode_share_access() implementation. A local,

unprivileged user could use this flaw to trigger a denial of service by creating a regular file on an NFSv4 (Network File System version 4) file system via mknod().

CVE-2011-4325, Moderate

A flaw was found in the Linux kernel's NFS implementation. A local, unprivileged user could use this flaw to cause a denial of service.

CVE-2011-4330, Moderate

A missing boundary check was found in the Linux kernel's HFS file system implementation. A local attacker could use this flaw to cause a denial of service or escalate their privileges by mounting a specially-crafted disk.

Red Hat would like to thank Kees Cook for reporting CVE-2011-1020, and Clement Lecigne for reporting CVE-2011-4330.

This update also fixes several bugs and adds one enhancement. Documentation for these bug fixes is available in the Red Hat Enterprise Linux 5.7 Technical Notes document:

https://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/html/5.7_Technical_Notes/kernel.html#RHSA-2012-0007

Users should upgrade to these updated packages, which contain backported patches to correct these issues, and fix the bugs and add the enhancement noted in the Technical Notes. The system must be rebooted for this update to take effect.

4.78.8. RHSA-2011:1479 — Important: kernel security, bug fix, and enhancement update

Updated kernel packages that fix multiple security issues, several bugs, and add one enhancement are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2011-1898, Important

Using PCI passthrough without interrupt remapping support allowed Xen hypervisor guests to generate MSI interrupts and thus potentially inject traps. A privileged guest user could use this flaw to crash the host or possibly escalate their privileges on the host. The fix for this issue can prevent PCI passthrough working and guests starting. Refer to Red Hat Bugzilla bug 715555 for details.

CVE-2011-3363, Moderate

A flaw was found in the way CIFS (Common Internet File System) shares with DFS referrals at their root were handled. An attacker on the local network who is able to deploy a malicious CIFS server could create a CIFS network share that, when mounted, would cause the client system to crash.

CVE-2011-4110, Moderate

A NULL pointer dereference flaw was found in the way the Linux kernel's key management facility handled user-defined key types. A local, unprivileged user could use the keyctl utility to cause a denial of service.

CVE-2011-1162, Low

A flaw in the way memory containing security-related data was handled in tpm_read() could allow a local, unprivileged user to read the results of a previously run TPM command.

CVE-2011-2203, Low

A NULL pointer dereference flaw was found in the Linux kernel's HFS file system implementation. A local attacker could use this flaw to cause a denial of service by mounting a disk that contains a specially-crafted HFS file system with a corrupted MDB extent record.

CVE-2011-2494, Low

The I/O statistics from the taskstats subsystem could be read without any restrictions. A local, unprivileged user could use this flaw to gather confidential information, such as the length of a password used in a process.

Red Hat would like to thank Yogesh Sharma for reporting CVE-2011-3363; Peter Huewe for reporting CVE-2011-1162; Clement Lecigne for reporting CVE-2011-2203; and Vasiliy Kulikov of Openwall for reporting CVE-2011-2494.

This update also fixes several bugs and adds one enhancement. Documentation for these bug fixes is available in the Red Hat Enterprise Linux 5.7 Technical Notes document:

https://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/html/5.7_Technical_Notes/kernel.html#RHSA-2011-1479

Users should upgrade to these updated packages, which contain backported patches to correct these issues, and fix the bugs and add the enhancement noted in the Technical Notes. The system must be rebooted for this update to take effect.

4.78.9. RHSA-2011:1386 — Important: kernel security, bug fix, and enhancement update

Updated kernel packages that fix multiple security issues, several bugs, and add one enhancement are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2011-2695, Important

The maximum file offset handling for ext4 file systems could allow a local, unprivileged user to cause a denial of service.

CVE-2011-2699, Important

IPv6 fragment identification value generation could allow a remote attacker to disrupt a target system's networking, preventing legitimate users from accessing its services.

CVE-2011-3191, Important

A malicious CIFS (Common Internet File System) server could send a specially-crafted response to a directory read request that would result in a denial of service or privilege escalation on a system that has a CIFS share mounted.

CVE-2011-1833, Moderate

A local attacker could use mount.ecryptfs_private to mount (and then access) a directory they would otherwise not have access to. Note: To correct this issue, the RHSA-2011:1241 ecryptfs-utils update must also be installed.

CVE-2011-2484, Moderate

A flaw in the taskstats subsystem could allow a local, unprivileged user to cause excessive CPU time and memory use.

CVE-2011-2496, Moderate

Mapping expansion handling could allow a local, unprivileged user to cause a denial of service.

CVE-2011-2723, Moderate

GRO (Generic Receive Offload) fields could be left in an inconsistent state. An attacker on the local network could use this flaw to cause a denial of service. GRO is enabled by default in all network drivers that support it.

CVE-2011-2942, Moderate

RHSA-2011:1065 introduced a regression in the Ethernet bridge implementation. If a system had an interface in a bridge, and an attacker on the local network could send packets to that interface, they could cause a denial of service on that system. Xen hypervisor and KVM (Kernel-based Virtual Machine) hosts often deploy bridge interfaces.

CVE-2011-3131, Moderate

A flaw in the Xen hypervisor IOMMU error handling implementation could allow a privileged guest user, within a guest operating system that has direct control of a PCI device, to cause performance degradation on the host and possibly cause it to hang.

CVE-2011-3188, Moderate

IPv4 and IPv6 protocol sequence number and fragment ID generation could allow a man-in-the-middle attacker to inject packets and possibly hijack connections. Protocol sequence number and fragment IDs are now more random.

CVE-2011-3209, Moderate

A flaw in the kernel's clock implementation could allow a local, unprivileged user to cause a denial of service.

CVE-2011-3347, Moderate

Non-member VLAN (virtual LAN) packet handling for interfaces in promiscuous mode and also using the be2net driver could allow an attacker on the local network to cause a denial of service.

CVE-2009-4067, Low

A flaw in the auerswald USB driver could allow a local, unprivileged user to cause a denial of service or escalate their privileges by inserting a specially-crafted USB device.

CVE-2011-1160, Low

A flaw in the Trusted Platform Module (TPM) implementation could allow a local, unprivileged user to leak information to user space.

CVE-2011-1585, Low

A local, unprivileged user could possibly mount a CIFS share that requires authentication without knowing the correct password if the mount was already mounted by another local user.

Red Hat would like to thank Fernando Gont for reporting CVE-2011-2699; Darren Lavender for reporting CVE-2011-3191; the Ubuntu Security Team for reporting CVE-2011-1833; Vasiliy Kulikov of Openwall for reporting CVE-2011-2484; Robert Swiecki for reporting CVE-2011-2496; Brent Meshier for reporting CVE-2011-2723; Dan Kaminsky for reporting CVE-2011-3188; Yasuaki Ishimatsu for reporting CVE-2011-3209; Somnath Kotur for reporting CVE-2011-3347; Rafael Dominguez Vega for reporting CVE-2009-4067; and Peter Huewe for reporting CVE-2011-1160. The Ubuntu Security Team acknowledges Vasiliy Kulikov of Openwall and Dan Rosenberg as the original reporters of CVE-2011-1833.

This update also fixes several bugs and adds one enhancement. Documentation for these bug fixes and the enhancement is available in the Red Hat Enterprise Linux 5.7 Technical Notes document:

https://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/html/5.7_Technical_Notes/kernel.html#RHSA-2011-1386

Users should upgrade to these updated packages, which contain backported patches to correct these issues and add this enhancement. The system must be rebooted for this update to take effect.

4.78.10. RHSA-2011:1212 — Important: kernel security and bug fix update

Updated kernel packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2011-2482, Important

Bug Fixes

A NULL pointer dereference flaw was found in the Linux kernel's Stream Control Transmission Protocol (SCTP) implementation. A remote attacker could send a specially-crafted SCTP packet to a target system, resulting in a denial of service.

CVE-2011-2491, Important

A flaw in the Linux kernel's client-side NFS Lock Manager (NLM) implementation could allow a local, unprivileged user to cause a denial of service.

CVE-2011-2517, Important

Buffer overflow flaws in the Linux kernel's netlink-based wireless configuration interface implementation could allow a local user, who has the CAP_NET_ADMIN capability, to cause a denial of service or escalate their privileges on systems that have an active wireless interface.

CVE-2011-2519, Moderate

A flaw was found in the way the Linux kernel's Xen hypervisor implementation emulated the SAHF instruction. When using a fully-virtualized guest on a host that does not use hardware assisted paging (HAP), such as those running CPUs that do not have support for (or those that have it disabled) Intel Extended Page Tables (EPT) or AMD Virtualization (AMD-V) Rapid Virtualization Indexing (RVI), a privileged guest user could trigger this flaw to cause the hypervisor to crash.

CVE-2011-2901, Moderate

An off-by-one flaw was found in the __addr_ok() macro in the Linux kernel's Xen hypervisor implementation when running on 64-bit systems. A privileged guest user could trigger this flaw to cause the hypervisor to crash.

CVE-2011-2495, Low

/proc/[PID]/io is world-readable by default. Previously, these files could be read without any further restrictions. A local, unprivileged user could read these files, belonging to other, possibly privileged processes to gather confidential information, such as the length of a password used in a process.

Red Hat would like to thank Vasily Averin for reporting CVE-2011-2491, and Vasiliy Kulikov of Openwall for reporting CVE-2011-2495.

This update also fixes several bugs. Documentation for these bug fixes is available in the Red Hat Enterprise Linux 5.7 Technical Notes document

https://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/html/5.7_Technical_Notes/kernel.html#RHSA-2011-1212

Users should upgrade to these updated packages, which contain backported patches to correct these issues, and fix the bugs noted in the Technical Notes. The system must be rebooted for this update to take effect.

4.79. kexec-tools

4.79.1. RHEA-2012:0090 — kexec-tools enhancement update

An updated kexec-tools package that adds one enhancement is now available for Red Hat Enterprise Linux 5.

The kexec-tools package contains the /sbin/kexec binary and utilities that together form the user-space component of the kernel's kexec feature. The /sbin/kexec binary facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. The kexec fastboot mechanism allows booting a Linux kernel from the context of an already running kernel.

Enhancement

BZ#772164

Kdump on Xen HVM guests is now enabled in Red Hat Enterprise Linux 5.7 as a Technology Preview. Performing a local dump to an emulated (IDE) disk using an Intel 64 Hypervisor with an Intel CPU is the only supported implementation. Note that the dump target must be specified in the /etc/kdump.conf file.

All users of kexec-tools are advised to upgrade to this updated package, which adds this enhancement.

4.79.2. RHSA-2012:0152 — Moderate: kexec-tools security, bug fix and enhancement update

An updated *kexec-tools* package that resolves three security issues, fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The *kexec-tools* package contains the **`/sbin/kexec`** binary and utilities that together form the user-space component of the kernel's kexec feature. The **`/sbin/kexec`** binary facilitates a new kernel to boot using the kernel's **`kexec`** feature either on a normal or a panic reboot. The **`kexec`** fastboot mechanism allows booting a Linux kernel from the context of an already running kernel.

Security Fixes

CVE-2011-3588

Kdump used the **`SSH`** (Secure Shell) **`StrictHostKeyChecking=no`** option when dumping to SSH targets, causing the target kdump server's SSH host key not to be checked. This could make it easier for a man-in-the-middle attacker on the local network to impersonate the kdump SSH target server and possibly gain access to sensitive information in the **`vmcore`** dumps.

CVE-2011-3589

The **mkdumprd** utility created **`initrd`** files with *world-readable* permissions. A local user could possibly use this flaw to gain access to sensitive information, such as the private SSH key used to authenticate to a remote server when **kdump** was configured to dump to an *SSH target*.

CVE-2011-3590

The **mkdumprd** utility included unneeded sensitive files (such as all files from the **`/root/.ssh/`** directory and the host's private SSH keys) in the resulting initrd. This could lead to an information leak when **`initrd`** files were previously created with *world-readable*

permissions. Note: With this update, only the SSH client configuration, known hosts files, and the SSH key configured via the newly introduced sshkey option in **/etc/kdump.conf** are included in the initrd. The default is the key generated when running the **service kdump propagate** command, **/root/.ssh/kdump_id_rsa**.

Red Hat would like to thank **Kevan Carstensen** for reporting these issues.

Bug Fixes

BZ#678308

On certain hardware, the *kexec kernel* incorrectly attempted to use a reserved memory range, and failed to boot with an error. This update adapts the underlying source code to determine the size of a backup region dynamically. As a result, **kexec** no longer attempts to use the *reserved memory range*, and boots as expected.

BZ#682359

The **mkdumprd** utility lacked proper support for using *VLAN devices over a bond interface*. Consequently, the network could not be correctly set up in the *kexec kernel* and **Kdump** failed to capture a core dump. This update modifies **mkdumprd** so it now provides full support for configuring VLAN devices over a bond interface. **Kdump** now successfully dumps the **vmcore** file to a remote machine in such a scenario.

BZ#759006

A bug in the **mkdumprd** caused **Kdump** to be unable to bring up a network interface card (NIC) if a NIC configuration file, such as **/etc/sysconfig/network-scripts/ifcfg-eth0**, did not contain a default gateway. When sending the **vmcore** file over a network using the **SSH** or **NFS** protocol, any attempt to bring the NIC up failed with the following error:

```
ifup: option with empty value "gateway"
```

Consequently, the connection to the remote machine could not be established and **Kdump** failed to dump the **vmcore** file. With this update, mkdumprd performs a check whether the default gateway is specified and thus avoids adding an empty gateway into the **/etc/kdump.conf** file. The **vmcore** file is now successfully dumped to a remote machine.

BZ#760844

A bug in **mkdumprd** caused **Kdump** to be unable to bring up a bridge device when its slave device was renamed in the kexec kernel. When sending the **vmcore** file over a *bridged network*, any attempt to bring the bridge device up failed with a similar error:

```
ifup: Ignoring unknown interface eth2
```

Consequently, the connection to the remote machine could not be established and Kdump failed to dump the **vmcore** file. This update modifies **mkdumprd** to search for the correct slave device names in NIC configuration files instead of using the old names. Kdump over a bridged network now works as expected.

BZ#761048

Certain storage devices, such as HP Smart Array 5i controllers using the **CCISS** driver, are known to be *non-resettable* in the kexec kernel. Therefore, when such a device was selected as a dump target, any attempt to dump a core file on it caused the *kexec kernel* to become unresponsive. This update modifies **mkdumprd** to check whether the target device is resettable. If the target device is non-resettable, then **Kdump** will not start and the kexec kernel no longer hangs under these circumstances.

BZ#761336

The **mkdumprd** utility was unable to handle errors returned by the **makedumpfile** command if the command was piped with other commands. Therefore, when sending a core dump file over a network using the SSH protocol and **makedumpfile** failed, the system *rebooted immediately* instead of dropping to the shell. This update allows **mkdumprd** to catch return codes of piped commands so that **Kdump** now fails right after a **makedumpfile** failure and the system drops correctly to the shell.

BZ#765702

The **mkdumprd** utility did not properly handle renaming of NIC devices in the kexec kernel. Therefore, when sending a core dump using a *VLAN device over a bond interface*, **Kdump** displayed various error messages related to VLAN device names. This update modifies **mkdumprd** so it now works with *VLAN device names* correctly.

BZ#781907

The **mkdumprd** utility did not handle *NFS unmount* failures correctly. Therefore, when dumping a core over the **NFS** protocol and a test attempt to unmount an NFS export failed, **mkdumprd** removed all files from this NFS export. This update corrects **mkdumprd** so that it only removes empty NFS exports and no data loss occurs under these circumstances.

Enhancements

BZ#668706

The **mkdumprd** utility lacked support for the **XFS** file system, and therefore **Kdump** failed to capture the vmcore dump file on XFS file systems. This update backports support for the **XFS** file system from Red Hat Enterprise Linux 6 so **Kdump** now creates core dumps on **XFS** file systems as expected.

BZ#690678

This update adds a new option for the **mkdumprd** utility, **blacklist**. This option allows **mkdumprd** to prevent specified kernel modules from being loaded into the **kexec** kernel.

BZ#715531

With this update, the **mkdumprd** utility supports *static route* configuration so that **Kdump** is now able to dump the **vmcore** file to a remote machine over a network with static routing.

BZ#719384

The **mkdumprd** utility has been modified to recognize and support **iSCSI** devices so that iSCSI devices can now be specified as a dump target.

BZ#743217

Kdump on **Xen** HVM guests is now enabled in Red Hat Enterprise Linux 5.8 as a Technology Preview. Performing a local dump to an emulated (IDE) disk using an Intel 64 **Hypervisor** with an Intel CPU is the only supported implementation. Note that the dump target must be specified in the **/etc/kdump.conf** file.

All users of *kexec-tools* are advised to upgrade to this updated package, which resolves these security issues, fixes these bugs and adds these enhancements.

4.80. krb5

4.80.1. RHSA-2011:1851 — Critical: krb5 security update

Updated krb5 packages that fix one security issue are now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having Critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

Kerberos is a network authentication system which allows clients and servers to authenticate to each other using symmetric encryption and a trusted third-party, the Key Distribution Center (KDC).

Security Fix

CVE-2011-4862

A buffer overflow flaw was found in the MIT krb5 telnet daemon (telnetd). A remote attacker who can access the telnet port of a target machine could use this flaw to execute arbitrary code as root.

Note that the krb5 telnet daemon is not enabled by default in any version of Red Hat Enterprise Linux. In addition, the default firewall rules block remote access to the telnet port. This flaw does not affect the telnet daemon distributed in the telnet-server package.

For users who have installed the krb5-workstation package, have enabled the telnet daemon, and have it accessible remotely, this update should be applied immediately.

All krb5-workstation users should upgrade to these updated packages, which contain a backported patch to correct this issue.

4.80.2. RHSA-2012:0306 — Low: krb5 security and bug fix update

Updated krb5 packages that fix one security issue and various bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

Kerberos is a network authentication system which allows clients and servers to authenticate to each other using symmetric encryption and a trusted third-party, the Key Distribution Center (KDC).

Security Fix

CVE-2011-1526

It was found that ftpd, a Kerberos-aware FTP server, did not properly drop privileges. On Red Hat Enterprise Linux 5, the ftpd daemon did not check for the potential failure of the effective group ID change system call. If the group ID change failed, a remote FTP user could use this flaw to gain unauthorized read or write access to files that are owned by the root group.

Red Hat would like to thank the MIT Kerberos project for reporting this issue. Upstream acknowledges Tim Zingelman as the original reporter.

Bug Fixes

BZ#701444

Due to a mistake in the Kerberos libraries, a client could fail to contact a Key Distribution Center (KDC) or terminate unexpectedly if the client had already more than 1024 file descriptors in use. This update backports modifications to the Kerberos libraries and the libraries use the poll() function instead of the select() function, as poll() does not have this limitation.

BZ#708516

The KDC failed to release memory when processing a TGS (ticket-granting server) request from a client if the client request included an authenticator with a subkey. As a result, the KDC consumed an excessive amount of memory. With this update, the code releasing the memory has been added and the problem no longer occurs.

BZ#713500

Under certain circumstances, if services requiring Kerberos authentication sent two authentication requests to the authenticating server, the second authentication request was flagged as a replay attack. As a result, the second authentication attempt was denied. This update applies an upstream patch that fixes this bug.

BZ#729067

Previously, if Kerberos credentials had expired, the klist command could terminate unexpectedly with a segmentation fault when invoked with the -s option. This happened when klist encountered and failed to process an entry with no realm name while scanning the credential cache. With this update, the underlying code has been modified and the command handles such entries correctly.

BZ#735363, BZ#736132

Due to a regression, multi-line FTP macros terminated prematurely with a segmentation fault. This occurred because the previously-added patch failed to properly support multi-line macros. This update restores the support for multi-line macros and the problem no longer occurs.

All users of krb5 are advised to upgrade to these updated packages, which resolve these issues.

4.81. ksh

4.81.1. RHBA-2012:0159 — ksh bug fix and enhancement update

An updated *ksh* package that fixes multiple bugs and adds one enhancement is now available for Red Hat Enterprise Linux 5.

KSH-93 is the most recent version of the *KornShell* by David Korn of AT&T Bell Laboratories. KornShell is a shell programming language which is also compatible with sh, the original Bourne Shell.

Bug Fixes

BZ#759498

When exiting a subshell after a command substitution, **ksh** could prematurely exit without any error. With this update, **ksh** no longer terminates under these circumstances and all subsequent commands are processed correctly.

BZ#743357

KornShell keeps a list of all non-zero return codes of old child processes with the list size limited by the *maximum number of child processes*. Previously, this list was not updated properly. Therefore, when PID numbers were reused on long running shells, **ksh** could erroneously return the exit code of the old process that had used the same PID number like the process that just exited. With this update **ksh** has been modified to ensure that the list of child processes return codes is updated properly, and the error no longer occurs in the scenario described.

BZ#739664

In **KSH-93**, when calling a function that was defined by using the **function** keyword, an additional subprocess was created, unlike for functions defined without this keyword. This update applies an upstream patch, which modifies behavior of **KSH-93** so that *no additional subprocesses* are created under these conditions.

BZ#736462

On Red Hat Enterprise Linux 5, not all kernel methods and user space utilities for file time stamps manipulation support *nanosecond resolution*. Previous **ksh** versions always used nanosecond resolution when comparing modification date of files. Therefore, when comparing files on **ext4** file systems, ksh returned unexpected results even though **ext4** file systems support nanosecond resolution. With this update, **ksh** has been modified to use only *second resolution* and file time stamps comparison now produces correct results in the scenario described.

BZ#736195, **BZ#709774**

Previously, when executing multiple piped commands within a script, there was a large *time window* between creating the child process and executing a command in the child process. This caused various problems with scripts relying on output of the **ps** command because the **ps** command detected more instances of the same script. With this update, this time window has been significantly reduced so the **ps** command now detects only one script instance.

BZ#698874

When running a script, the previous version of **ksh** could incorrectly consider the **eval** command to be the last in the script, and did not run it in a separate process. Consequently, using **eval** or executing commands from another file (that is, by using the **.** built-in command)

may have prevented **ksh** from executing any subsequent commands. With this update, the underlying source code has been adapted to determine whether a script contains other commands and to perform the selected action in a separate process if it does. As a result, **ksh** now executes all commands in a script as expected.

BZ#690816

Previously, **ksh** treated an *array declaration* as a definition. Consequently, the array contained one element after the declaration. This bug has been fixed, and now an array is correctly reported as *empty* after a declaration.

BZ#683722, BZ#727891

If the **IFS** variable was unset inside a function used in a script, the memory being used was erroneously freed. Consequently, **ksh** terminated unexpectedly with a segmentation fault. With this update, **ksh** allows the **IFS** variable to be unset, but without freeing the memory so that **ksh** no longer crashes under these circumstances.

BZ#616853

Assigning a value to an array variable during the execution of the **typeset** command could cause **ksh** to terminate unexpectedly with a *segmentation fault*. This update corrects the array handling in this command and **ksh** no longer crashes.

BZ#586923

Due to a memory leak in the **ksh** executable, the performance of *long running scripts* could decrease significantly over time. With this update, the underlying source code has been modified to prevent this memory leak, and the execution of long running scripts is no longer slowed down.

BZ#691933

In POSIX functions, a function defined without using the **function** keyword, the value of the variable **$0** was changed to the name of the function instead of keeping the original value, the name of the caller function. With this update, an upstream patch has been applied to correct the code and **ksh** keeps the name of the caller function in **$0** as expected.

BZ#642508

Prior to this update, **ksh** did not close a file containing an *auto-loaded* function definition. After loading several functions, **ksh** could have easily exceeded the system's limit on the number of open files. With this update, files containing auto-loaded functions are properly closed, thus, the number of opened files no longer increases with usage.

BZ#615284

When a **ksh** script contained the **trap** command to capture a **SIGPIPE** signal, sending this signal via the built-in **echo** command could cause its output to be incorrectly added to the redirected output of an external command. With this update, **ksh** now flushes the output buffer before redirecting any output streams.

BZ#601555

Due to incorrect signal handling, receiving a signal while still processing the previously sent

signal caused **ksh** to terminate unexpectedly with a *segmentation fault*. With this update, the subsequent signals are deferred until the current signal is processed; thus, **ksh** no longer crashes.

BZ#743302

Previously, **ksh** became unresponsive when pipes were used in an **`eval`** argument. With this update, an upstream patch has been applied and the **ksh** no longer hangs in the scenario described.

BZ#712349

Previously, the **`ulimit`** built-in function did not properly handle setting of the limit for virtual memory usage, which was set by the **`-v`** parameter. Consequently, every time this limit was modified, also the *CPU time limit* was changed, which was undesirable. This update modifies handling of the *virtual memory limit* so that it does not influence the CPU time limit anymore.

BZ#699823, BZ#726199

When running a **ksh** script, the exit code of a child process was not preserved. Consequently, when a script asked for such an exit code, the wrong value was reported. With this update, **ksh** now stores exit codes of child processes so that the exit codes are available for the future use.

BZ#659459

When a **ksh** script created a file and immediately opened it after the creation, the operation failed. This happened because, in some cases, the file being created did not exist yet. With this update, this race condition has been fixed and once a file is created, it is immediately available for any following commands.

BZ#647524

File name completion used after an environment variable failed and **ksh** reported a bad substitution error. With this update, an upstream patch has been applied which fixes the problem.

BZ#640379

Previously, **ksh** did not always wait for a **`pipeline`** to complete when the **`pipefail`** option was used. Consequently, a *failed exit status* was erroneously reported even when the **`pipeline`** had not failed. With this update, the code has been improved and the **`pipefail`** option now functions as expected.

BZ#584704

In **ksh**, when performing *nested command substitution*, each command is performed in a separate **`coprocess`**. The previous version of **ksh** did not handle the nested command substitutions correctly, which could result in a race condition between *job routines* in the *signal handler* and the *parent process*. Subsequently, **ksh** could erroneously close stdout of the running coprocess. With this update, **ksh** now checks whether the coprocess is running before it attempts to close its file descriptor. **KornShell** now handles the nested command substitutions properly.

BZ#650998

Previously, **ksh** did not restore *file handles* after executing a sourced script. If an **output stream** or an **error stream** was redirected in the sourced script, the respective stream remained redirected in the *parent script* as well. With this update, file handles are restored after execution of sourced scripts so a parent script is not affected by sourced script redirections.

BZ#644128

If a **here** document (**heredoc** - specifies a string literal in command line shells) was combined with an *auto-loaded* function, interference with the **here** document processing could occur causing output to be truncated to **8 KB**. This update improves the **here** document processing logic and auto-loaded functions no longer have a negative side effect on **here** documents.

BZ#587127

As a result of a previous code optimization, the **whence** built-in command could enter an infinite loop when used with the **-q** option. Consequently, **ksh** consumed up to **100% of CPU** and became unresponsive. With this version of **ksh**, the underlying code of the **whence** built-in command has been modified and **ksh** no longer hangs, when **-q** option is used.

BZ#573936

When performing certain operations, such as reading the user's input, **ksh** switches the terminal into **raw mode** with *echo* disabled. Normally, the terminal is restored with the previous settings after the operation has been finished. This did not work in the previous **ksh** version if the user's **locale** was set to use *multibyte encoding* (for example **UTF-8**). With such a locale, **ksh** failed to restore the terminal settings if it timed out while executing the **read** built-in command. Subsequently, the terminal did not echo any characters until it was reset. This updates applies a patch ensuring that the terminal is restored properly after timeout and user's input is now echoed as expected.

BZ#691850

The **kill** built-in command did not properly handle errors when it was given an extremely large value as the PID parameter. The **kill** command then internally reported the code **-1**, which was interpreted by **ksh** as the **-1** option and **ksh** thus killed all user processes. This update corrects handling of PID conversion errors so that **ksh** can no longer misinterpret the **kill** command return values. The command now, under these circumstances, fails with an error as expected.

Enhancements

BZ#574867

The **ksh** built-in **ulimit** command now provides the ability to read and set the **RLIMIT_RTPRIO** and **RLIMIT_NICE** resource limiters.

All users of *ksh* are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.82. kudzu

4.82.1. RHEA-2012:0232 — kudzu bug fix and enhancement update

An updated kudzu package that fixes one bug and adds one enhancement is now available for Red Hat Enterprise Linux 5.

Kudzu is a hardware probing library for automatic discovery and configuration of hardware.

Bug Fix

BZ#695388

Kudzu classified InfiniBand devices as "OTHER" so that the Anaconda installer did not recognize these devices and did not create respective network interfaces. With this update, Kudzu correctly detects InfiniBand devices as "NETWORK" devices so Anaconda can create network interfaces accordingly.

Enhancement

BZ#717889

This update adds support for Fusion-io ioDrive devices so these devices are now detected by Kudzu and can be used and configured by Anaconda.

All users of kudzu are advised to upgrade to this updated package, which fixes this bug and adds this enhancement.

4.83. kvm

4.83.1. RHSA-2012:0051 — Important: kvm security update

Updated kvm packages that fix two security issues are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel.

Security Fixes

CVE-2012-0029

A heap overflow flaw was found in the way QEMU-KVM emulated the e1000 network interface card. A privileged guest user in a virtual machine whose network interface is configured to use the e1000 emulated driver could use this flaw to crash the host or, possibly, escalate their privileges on the host.

CVE-2011-4622

A flaw was found in the way the KVM subsystem of a Linux kernel handled PIT (Programmable Interval Timer) IRQs (interrupt requests) when there was no virtual interrupt controller set up. A malicious user in the kvm group on the host could force this situation to occur, resulting in the host crashing.

Red Hat would like to thank Nicolae Mogoreanu for reporting CVE-2012-0029.

All KVM users should upgrade to these updated packages, which contain backported patches to correct these issues. Note: The procedure in the Solution section must be performed before this update will take effect.

4.83.2. RHSA-2012:0149 — Moderate: kvm security, bug fix and enhancement update

Updated *kvm* packages that resolve one security issue, and fix several bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

KVM (Kernel-base Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel.

Security Fixes

CVE-2011-4347

It was found that the **`kvm_vm_ioctl_assign_device()`** function in the KVM subsystem of a Linux kernel did not check if the user requesting device assignment was privileged or not. A member of the kvm group on the host could assign unused PCI devices, or even devices that were in use and whose resources were not properly claimed by the respective drivers, which could result in the host crashing.

Red Hat would like to thank Sasha Levin for reporting this issue.

Bug Fixes

BZ#700281

Due to leaking file descriptors, if a Network Interface Card (NIC) was attached to or detached from a guest machine more than 250 times, **KVM** failed with the following error message:

```
get_real_device: /sys/bus/pci/devices/0000:09:00.0/resource: Too many open
files
```

The problem has been fixed, and NIC can now be successfully attached to or detached from a guest machine more than 250 times.

BZ#701616

When booting a guest with more than 8 PCI devices, QEMU exits with the following message:

```
Too many assigned devices
```

However, when hot plugging PCI devices, the limitation of maximum number of devices assigned did not take effect, and the user could hot plug more than 8 PCI devices. **QEMU** has been modified to refuse to assign the ninth and any further hot plugged PCI devices with the aforementioned error message.

BZ#703335

Previously, the **mktime()** function incorrectly modified an input parameter according to the time zone of the host machine. As a consequence, if the user did not use Network Time Protocol (NTP) and the time zone on the host machine was set to "America/New_York", time displayed on the clock of a guest machine was shifted one hour forward on the first reboot. With this update, **mktime()** is not used if UTC time is specified, and the correct time is displayed in the aforementioned scenario.

BZ#703446

When the user booted a guest machine with a virtual Intel e1000 network interface card (NIC) and changed the maximum transmission unit (MTU) value, the guest machine could not be pinged from the host machine. With this update, multi-buffer packets are now supported, and the guest machine can be pinged successfully.

BZ#704081

Previously, variables that represented RAM addresses were declared as the "long" data type. Large numbers (guests with large memory defined) could lead to overflow, and consequently cause screen corruption or cause the utility to terminate unexpectedly with a segmentation fault. With this update, variables that represent RAM addresses are declared as the "ram_addr_t" data type, and the aforementioned problems no longer occur on guests with large memory defined.

BZ#725629

Previously, asynchronous I/O (aio) threads were created by threads of the virtual CPU. If the affinity of the virtual CPU was set, asynchronous I/O threads inherited this affinity. This could, in certain cases, lead to unexpectedly high latency of the virtual machines. With this update, asynchronous I/O threads are created by the main thread, and therefore inherit the main thread's affinity instead of the affinity of the virtual CPU. This ensures proper responses of virtual machines.

BZ#725876

Previously, the kvm utility did not properly emulate the real-time clock (RTC) alarm interrupts (AIE) on host machines running Red Hat Enterprise Linux 5. Newer kernels use AIE interrupts exclusively for RTC functionality (including update interrupt, or UIE, mode). As a consequence, if the user ran a guest machine with a recent kernel on the Red Hat Enterprise Linux 5 host, various bugs could manifest. Among these, for example, the following message could appear when running the hwclock utility:

```
select() to /dev/rtc to wait for clock tick timed out
```

This update adds support for the AIE mode emulation, so that UIE and AIE mode interrupts now work properly and applications run as expected.

BZ#751482

During the boot process inside the **qemu-kvm** utility, the screen was resized to the height of 1. A mouse click at this point caused a division by zero (the SIGFPE signal was sent) when calculating the absolute position of the pointer from the pixel. As a consequence, qemu-kvm terminated with the "Floating point exception" error. With this update, mouse click coordinates are forced to return values from the middle of the screen, so that qemu-kvm no longer

terminates in the described scenario.

All **KVM** users should upgrade to these updated packages, which contain backported patches to correct this issue and fix these bugs.

Important

The following procedure must be performed before this update will take effect:

1. Stop all KVM guest virtual machines.
2. Either reboot the hypervisor machine or, as the root user, remove (using "modprobe -r [module]") and reload (using "modprobe [module]") all of the following modules which are currently running (determined using "lsmod"): kvm, ksm, kvm-intel or kvm-amd.
3. Restart the KVM guest virtual machines.

4.84. less

4.84.1. RHBA-2011:1468 — less bug fix update

An updated less package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The less package contains a text file browser that is similar to the more browser, but with more features ("less is more"). The less text file browser allows users to move backwards in the file as well as forwards. Because the less utility does not need to read the entire input file before it starts, it starts up faster than text editors.

* Prior to this update, a debuginfo file for a binary was missing from the less-debuginfo package. As a result, the crash analysis via the Automatic Bug-Reporting Tool (ABRT) did not work as expected and debugging via GNU Debugger (GDB) could fail. This update modifies the spec file so that the crash analysis via ABRT and debugging via GDB work as expected. (BZ#734827)

4.85. lftp

4.85.1. RHBA-2011:1541 — lftp bug fix update

An updated lftp package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

LFTP is a sophisticated file transfer program for the FTP and HTTP protocols. Like bash, it has job control and uses the readline library for input. It has bookmarks, built-in mirroring, and can transfer several files in parallel. It is designed with reliability in mind.

Bug Fixes

BZ#532099

The GnuTLS library does not support some previously offered TLS ciphers. As a consequence, some users experienced the error message, "Fatal error: gnutls_handshake: A TLS fatal alert has been received", when attempting to use SSL. With this update, it is now possible to force an SSLv3 connection instead of TLS using the "set ftp:ssl-auth SSL" configuration directive for servers without support for any of the TLS ciphers listed. This works both for implicit and explicit FTPS.

BZ#570495

Prior to this update, the lftp client was not able to support "CLEAR COMMAND CHANNEL" (CCC) mode (RFC4217). Without CCC, Layer 7 aware firewalls cannot see the PASV port statements necessary to open the requisite data ports for transfers. This updated package fixes the described weakness and the lftp client supports CCC mode as intended. As a result data transfers through Layer 7 aware firewalls no longer fail in the scenario described.

BZ#727435

Prior to this update, when the lftp client was started with the "-e" option and the mget command was used, the returned exit status code was zero, (success), when creating a connection to a URL had failed due to the specified URL being non-existent. This update applies a patch that improves the error handling in mget. As a result, the lftp client now returns exit status code '1', indicating a failure, when creating a connection fails in the scenario described.

All users of lftp are advised to upgrade to this updated package, which fixes these bugs.

4.86. libcxgb3

4.86.1. RHBA-2012:0184 — libcxgb3 bug fix and enhancement update

updated libcxgb3 packages that fix various bugs and add multiple enhancements are now available for Red Hat Enterprise Linux 5.

The libcxgb3 packages provide a userspace hardware driver for the libibverbs InfiniBand/iWARP verbs library. This driver enables Chelsio iWARP capable ethernet devices.

The libcxgb3 package has been upgraded to upstream version 1.3.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#717437)

All users of libcxgb3 are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.87. libdhcp

4.87.1. RHBA-2012:0193 — libdhcp bug fix update

Updated libdhcp packages that fix three bugs are now available for Red Hat Enterprise Linux 5.

libdhcp enables programs to invoke and control the Dynamic Host Configuration Protocol (DHCP) clients: the Internet Software Consortium (ISC) Internet Protocol version 4 (IPv4) DHCP client library, libdhcp4client, and the Internet Protocol version 6 (IPv6) DHCPv6 client library, libdhcp6client.

Bug Fix

BZ#599633

Prior to this update, interface card (NIC) indexes were interrupted internally due to a cache iteration error in libdhcp. The update ensures that the interfaces are enumerated sequentially so that there are no index gaps. Now, libdhcp works as expected.

BZ#616865

Prior to this update, interfaces that were enabled at boot time had, under certain circumstances, invalid flags like DEBUG PROMISC or ALLMULTI. This update no longer passes these flags.

BZ#737155

Prior to this update, the libdhcp timeout was not correctly passed. As a result certain requests always stopped after 60 seconds even if the corresponding command line option allowed for more time. This update correctly passes the dhcp timeout value to the dhcp client library. This update is a dependency of BZ#736515 and BZ#737161.

All users of libdhcp are advised to upgrade to these updated packages, which fix these bugs.

4.88. libexif

4.88.1. RHBA-2011:1472 — libexif bug fix update

An updated libexif package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The libexif package provides a library for reading and extracting image metadata from Exif image files.

Bug Fix

BZ#689614

When opening an invalid or corrupt Exif file, libexif allocated huge amounts of memory. This could cause a memory exhaustion situation and the system then became unresponsive, which eventually resulted in a crash of the running graphics application, such as Gimp. The libexif code has been modified to check validity of the Exif file before it allocates the memory. Memory is now allocated properly and graphic programs no longer crash under these circumstances.

All users of libexif are advised to upgrade to this updated package, which fixes this bug.

4.89. libhbaapi

4.89.1. RHBA-2011:1425 — libhbaapi package updated

An updated libhbaapi package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The libhbaapi library is the Host Bus Adapter (HBA) API library for Fibre Channel and Storage Area Network (SAN) resources. It contains a unified API that programmers can use to access, query, observe and modify SAN and Fibre Channel services.

Bug Fixes

BZ#747897

The "libHBAAPI.so" shared object library, which provides the Host Bus Adapter API library, failed to define a build dependency on the "libdl.so" library. As a result, applications that linked to "libHBAAPI.so" without themselves including the "libdl.so" dependency failed at start time when the libHBAAPI library tried to call the dlopen function. With this update, the libdl.so dependency has been added and the application builds as expected.

BZ#747897

Prior to this update, hba.conf was not marked in the libhbaapi package specification file (spec file) as being exempt from verification. Consequently, if the hba.conf config file was changed it was reported as an error by the file verify function "rpm -V libhbaapi". With this update hba.conf is now marked in the spec file as "%verify(not md5 size mtime)". As a result the hba.conf file is no longer erroneously verified (for size, mtime, and checksum) and the test functions as expected in the scenario described.

All users of libhbaapi are advised to upgrade to this updated package, which fixes these bugs.

4.90. libmlx4

4.90.1. RHBA-2012:0270 — libmlx4 bug fix update

Updated libmlx4 packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The libmlx4 packages provide a device-specific user space driver for Mellanox ConnectX InfiniBand adapter cards for use with the libibverbs library.

Bug Fix

BZ#709987

Prior to this update, editing the /etc/ofed/mlx4.conf configuration file to change a port on a Mellanox ConnectX InfiniBand host channel adapter (HCA) to "eth" (Ethernet) could cause various errors to occur. This update corrects this error, and such a port can now be changed as expected.

All users of Mellanox ConnectX InfiniBand adapter cards are advised to upgrade to these updated packages, which fix this bug.

4.91. libpng

4.91.1. RHSA-2011:1104 — Moderate: libpng security update

Updated libpng packages that fix two security issues are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The libpng packages contain a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files.

Security Fixes

CVE-2011-2690

A buffer overflow flaw was found in the way libpng processed certain PNG image files. An attacker could create a specially-crafted PNG image that, when opened, could cause an application using libpng to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

Note

The application behavior required to exploit CVE-2011-2690 is rarely used. No application shipped with Red Hat Enterprise Linux behaves this way, for example.

CVE-2011-2692

An uninitialized memory read issue was found in the way libpng processed certain PNG images that use the Physical Scale (sCAL) extension. An attacker could create a specially-crafted PNG image that, when opened, could cause an application using libpng to crash.

Users of libpng should upgrade to these updated packages, which contain backported patches to correct these issues. All running applications using libpng must be restarted for the update to take effect.

4.92. libusb

4.92.1. RHBA-2011:1498 — libusb bug fix

An updated libusb package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The libusb package provides a way for applications to access USB devices.

Bug Fix

BZ#634915

Prior to this update, installing libusb-devel packages of two different architectures in a multilib environment failed. An error occurred due to one architecture independent file (manual.ps) differing between the packages being installed. With this update, creation timestamps are removed from manual.ps so that the file is the same in each package. As a result installation of libusb-devel packages for two different architectures now succeeds.

All users of libusb are advised to upgrade to this updated package, which resolves this issue.

4.93. libvirt

4.93.1. RHBA-2012:0248 — libvirt bug fix update

Updated libvirt packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems. In addition, libvirt provides tools for remote management of virtualized systems. The libvirt library also provides nwfilter support for fine-grained filtering of the network traffic reaching guests managed by libvirt.

Bug Fixes

BZ#676622

Prior to this update, the automatic IPTables rule that allowed Trivial File Transfer Protocol

(TFTP) traffic could cause the libvirt daemon (libvirtd) to report errors after upgrading the daemon. This update removes the rule after tftp was added.

BZ#719435

Prior to this update, the target tag that indicates which host is allowed to see the the list of disks to be exported to the guests was ignored and the disks were named in the order they appeared in the XML file instead. This update modifies the order of disks and controllers so that the target tag is no longer ignored.

BZ#735127

Prior to this update, the dclose() function invoked an already removed callback function if the thread local remained in the memory. As a consequence, libvirt terminated unexpectedly with a segmentation fault when unloading the libvirt.so provider. This update links libvirt with with the -z nodelete option to prevent the code from being removed from memory when calling dlclose().

BZ#747514

Prior to this update, the Coverity check contained several defects that could mask security driver failures, fail to configure the mac_filter, leak resources using domxml-from-native options. This update modifies the underlying code so that these defects no longer occur.

BZ#771720

Prior to this update, the QEMU driver could fail to find the user or group ID of the QEMU application on the system due to a programming error in the initialization code of libvirtd. As a result, libvirtd could fail to start. This update modifies the initialization code and libvirtd now works as expected.

All users of libvirt are advised to upgrade to these updated packages, which fix these bugs.

4.94. libvorbis

4.94.1. RHSA-2012:0136 — Important: libvorbis security update

Updated libvorbis packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The libvorbis packages contain runtime libraries for use in programs that support Ogg Vorbis. Ogg Vorbis is a fully open, non-proprietary, patent-and royalty-free, general-purpose compressed audio format.

Security Fix

CVE-2012-0444

A heap-based buffer overflow flaw was found in the way the libvorbis library parsed Ogg Vorbis media files. If a specially-crafted Ogg Vorbis media file was opened by an application using libvorbis, it could cause the application to crash or, possibly, execute arbitrary code with the

privileges of the user running the application.

Users of libvorbis should upgrade to these updated packages, which contain a backported patch to correct this issue. The desktop must be restarted (log out, then log back in) for this update to take effect.

4.95. libX11

4.95.1. RHBA-2011:1351 — libX11 bug fix update

An updated libX11 package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The libX11 package contains the core X11 protocol client library.

Bug Fix

BZ#736175

Previously, in the 64-bit mode, libX11 computed addresses using the 32-bit arithmetic. As a consequence, under heavy load, applications running in the X environment terminated unexpectedly. A patch has been provided to address this issue, and the crashes no longer occur in the described scenario.

Users of libX11 are advised to upgrade to this updated package, which fixes this bug.

4.96. libXcursor

4.96.1. RHBA-2011:1538 — libXcursor bug fix update

An updated libXcursor package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The X.Org's X11 libXcursor runtime library for cursor management.

Bug Fix

BZ#688657

Prior to this update, libXcursor allocated memory to store the comment and fileheader associated with the cursor data but due to an inversion in the logic, which would not free the memory if the associated pointer was not NULL, this allocated memory was never freed. Consequently this caused a memory leak each time a cursor was created or loaded with libXcursor. This update fixes the internal logic, the data is freed as required when the pointer is set, and the memory leaks no longer occur in the scenario described.

All users of libXcursor are advised to upgrade to this updated package, which fixes this bug.

4.97. libXfont

4.97.1. RHSA-2011:1154 — Important: libXfont security update

Updated libXfont packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The libXfont packages provide the X.Org libXfont runtime library. X.Org is an open source implementation of the X Window System.

Security Fix

CVE-2011-2895

A buffer overflow flaw was found in the way the libXfont library, used by the X.Org server, handled malformed font files compressed using UNIX compress. A malicious, local user could exploit this issue to potentially execute arbitrary code with the privileges of the X.Org server.

Users of libXfont should upgrade to these updated packages, which contain a backported patch to resolve this issue. All running X.Org server instances must be restarted for the update to take effect.

4.98. libxml2

4.98.1. RHSA-2012:0017 — Important: libxml2 security update

Updated libxml2 packages that fix several security issues are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The libxml2 library is a development toolbox providing the implementation of various XML standards. One of those standards is the XML Path Language (XPath), which is a language for addressing parts of an XML document.

Security Fixes

CVE-2011-3919

A heap-based buffer overflow flaw was found in the way libxml2 decoded entity references with long names. A remote attacker could provide a specially-crafted XML file that, when opened in an application linked against libxml2, would cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2011-0216

An off-by-one error, leading to a heap-based buffer overflow, was found in the way libxml2 parsed certain XML files. A remote attacker could provide a specially-crafted XML file that, when opened in an application linked against libxml2, would cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2011-1944

An integer overflow flaw, leading to a heap-based buffer overflow, was found in the way libxml2 parsed certain XPath expressions. If an attacker were able to supply a specially-crafted XML file to an application using libxml2, as well as an XPath expression for that application to run against the crafted file, it could cause the application to crash or, possibly, execute arbitrary

code.

CVE-2010-4008, **CVE-2011-2834**

Flaws were found in the way libxml2 parsed certain XPath expressions. If an attacker were able to supply a specially-crafted XML file to an application using libxml2, as well as an XPath expression for that application to run against the crafted file, it could cause the application to crash.

CVE-2011-3905

An out-of-bounds memory read flaw was found in libxml2. A remote attacker could provide a specially-crafted XML file that, when opened in an application linked against libxml2, would cause the application to crash.

Note

Red Hat does not ship any applications that use libxml2 in a way that would allow the CVE-2011-1944, CVE-2010-4008, and CVE-2011-2834 flaws to be exploited; however, third-party applications may allow XPath expressions to be passed which could trigger these flaws.

Red Hat would like to thank the Google Security Team for reporting the CVE-2010-4008 issue. Upstream acknowledges Bui Quang Minh from Bkis as the original reporter of CVE-2010-4008.

All users of libxml2 are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The desktop must be restarted (log out, then log back in) for this update to take effect.

4.98.2. RHBA-2011:1416 — libxml2 bug fix update

Updated libxml2 packages that resolve an issue are now available for Red Hat Enterprise Linux 5.

The libxml2 library provides a development tool to manipulate XML and HTML files. The library also implements various XML and HTML standards. One of those standards is XML Schemas which allows validation of the content of an XML document.

Bug Fix

BZ#747865

The libxml2 XML Schemas implementation allowed empty values for integer fields using, for example, the predefined schemas type, xsd:byte. This led to unwanted validation of documents that were invalid per these schemas. The implementation has been modified to forbid those empty integer values, and all documents containing such values will now fail the XML Schemas validation.

All users of libxml2 are advised to upgrade to these updated packages, which fix this bug.

4.99. lsof

4.99.1. RHBA-2012:0206 — lsof bug fix and enhancement update

An updated lsof package that fixes two bugs and adds two enhancements is now available for Red Hat Enterprise Linux 5.

The lsof (LiSt Open Files) package provides a utility to list information about files that are open and running on Linux and UNIX systems.

Bug Fixes

BZ#513613

Prior to this update, the lsof utility ignored the -w option if both the -b and the -w options were specified. As a consequence, lsof failed to suppress warning messages. This update modifies the %changelog section of the underlying code. Now, the -w option successfully suppresses warning messages.

BZ#705424

Prior to this update, lsof could, under certain circumstances, report incorrect server locations of mounted folders if multiple Network File System (NFS) shares from one host were mounted. This update allows multiple NFS clients to share superblocks. Now, lsof reports the correct server locations of mounted folders.

Enhancements

BZ#582672

This update adds offset support to report file offset of opened files.

BZ#733684

This update adds the new option +|-e s to lsof which exempts file systems with the path name "s" from being subjected to kernel function calls that can block.

All users of lsof are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.100. ltrace

4.100.1. RHBA-2011:1473 — ltrace bug fix update

An updated ltrace package that fixes various bugs is now available.

The ltrace utility is a debugging program that runs a specified command until the command exits. While the command is executing, ltrace intercepts and records both the dynamic library calls called by the executed process and the signals received by the executed process. The ltrace utility can also intercept and print system calls executed by the process.

Bug Fix

BZ#733216

When tracing a process with many threads, the traced process would very likely be killed as the threads ran into breakpoins that wouldn't be handled by ltrace. With this update, ltrace attaches to the newly created threads, and carefully handles the breakpoints so that tracing events are not missed.

Note: when ltrace attached to a running process, that process could have been detached with the instruction pointer pointed mid-instruction, or with pending events, which would kill the process. This update improves the detach logic so that the process is left in a consistent state before detaching.

All users of ltrace are advised to upgrade to this updated package, which resolves these issues.

4.101. lvm2

4.101.1. RHBA-2012:0056 — lvm2 bug fix update

An updated lvm2 package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The lvm2 package provides support for Logical Volume Management (LVM).

Bug Fix

BZ#773587

Due to an incorrect test condition in the underlying code, lvm operations could enter an infinite loop if the system contained 4 or more volume groups with duplicate names. With this update, the erroneous test condition has been corrected and lvm commands now complete as expected in this scenario.

All users of lvm2 are advised to upgrade to this updated package, which fixes this bug.

4.101.2. RHBA-2011:1222 — lvm2 bug fix update

An updated lvm2 package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The lvm2 package provides support for Logical Volume Management (LVM).

Bug Fix

BZ#732006

When running the "lvconvert" command to convert a linear device to a mirror with stripes, the "lvconvert" command entered an infinite loop.The problem occurred if the number of needed extents was not divisible by the number of areas. This has been fixed: the allocation is now properly rejected if the number of extents is not divisible by the number of areas.

All users of lvm2 are advised to upgrade to this updated package, which fixes this bug.

4.101.3. RHBA-2012:0161 — lvm2 bug fix and enhancement update

An updated *lvm2* package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 5.

The *lvm2* package contains support for Logical Volume Management (LVM).

Upgrade to an upstream version

The *lvm2* package has been upgraded to upstream version 2.02.88, which provides a number of bug fixes and enhancements over the previous version. (BZ#746302)

Bug Fixes

BZ#597010

LVM no longer scans multipath member devices (underlying paths for active multipath devices) and prefers top-level devices. This new default behavior can be switched off using the ***multipath_component_detection*** option in the **/etc/lvm/lvm.conf** file.

BZ#636991

Prior to this update, placing mirror images on different physical devices with the **lvcreate --alloc anywhere** command did not guarantee placement of data on different physical devices. With this update, the above command tries to allocate each mirror image to a separate device first before placing it on a device that is already used.

BZ#702065

LVM mirrors can be operated in *single-machine* or *cluster-aware* mode. The cluster-aware mode requires a service daemon and an additional kernel module. HA-LVM makes use of the single-machine mode and should not require the extra daemon or module as long as the LVM mirrors are active exclusively. When a volume was being repaired or converted using the **lvconvert** command, the exclusive nature of the activation was lost and the cluster-aware mode was attempted. This failed due to the lack of the necessary daemon or kernel module. The following error message was logged:

```
Unable to send cluster log request [DM_CLOG_CTR] to server: -3
```

Consequently, mirrors managed by HA-LVM were unable to handle device failures. The commands that are used to repair or convert LVM mirrors have been fixed in order to preserve exclusive activation. This ensures that only the single-machine kernel representation is used and the extra daemon and kernel module necessary for cluster-aware operation, which may not be present, are not invoked. As a result the **lvconvert** command now works correctly in the scenario described.

BZ#706036

Any I/O operations sent to an underlying device while it is suspended are queued and will not complete until the device is resumed. When running the **pvmove** utility on a Logical Volume (LV), **pvmove** sometimes became unresponsive trying to suspend a device when the underlying device was already suspended and had I/O operations pending. The code for **pvmove** has been improved and **pvmove** now temporally resumes all the underlying LVs before trying to suspend an LV in order to allow any I/O operations to complete.

BZ#707056

The automatic snapshot resize process was reported to have finished twice by **dmeventd**, the event monitoring daemon for device-mapper devices. The code has been improved and the redundant information after a resize operation is no longer logged to system log.

BZ#707779

When running the **lvconvert** command to convert a linear device to a mirror with stripes, the **lvconvert** command entered an infinite loop. The problem occurred if the number of needed extents was not divisible by the number of areas. This has been fixed: the allocation is now properly rejected if the number of extents is not divisible by the number of areas.

BZ#708444

The automatic extension of volumes was reported by **dmeventd** when they were being written to and filling up even when the threshold was turned off by setting **snapshot_autoextend_threshold = 100**. This update removes this message as it is now considered redundant because the LVM command **lvextend** reports all relevant information.

BZ#711185

Prior to this update, extending a mirror volume beyond available extents while using the cling-by-tags allocation policy did not work properly. Normally, such an action returns an error message informing the user that there are insufficient allocatable extents for use. However, this check failed and caused a volume to be corrupted. Because the allocation code has been revised, restructured, and made more robust, the problematic scenario with extending mirror volumes while using the cling-by-tags policy no longer occurs.

BZ#719760

If an MD linear device had set rounding using the overloaded chunk size attribute, the **pvcreate** command logged the following erroneous error:

```
/dev/md0 sysfs attr level not in expected format: linear
```

This update removes the unnecessary warning in **pvcreate** for MD linear devices.

BZ#745522

In some circumstances, when running **lvm** reporting commands and a physical volume was not specified, the following error message appeared:

```
dm_report: left-aligned snprintf() failed
```

The memory allocation code has been improved and this error no longer appears.

BZ#749650

When using striped mirrors, improper and overly-restrictive divisibility requirements for the extent count could cause a failure to create a striped mirror, even though it was possible. The condition that was checked took account of the mirror count and the stripe count, when the stripe count alone was satisfactory. This update corrects the code, and creating a striped mirror no longer fails in the scenario described.

BZ#755762

Splitting an LV between two volume groups failed when the mirrored volumes had logs which were also mirrored. With this update, the **vgsplit** command is now able to split a volume

group containing a mirror with mirrored logs.

BZ#769053

If preallocated memory was too low, *lvm2* issued the following error message:

```
Internal error: Maps lock < unlock
```

The message has been changed to a message in the following format:

```
Reserved memory (%ld) not enough: used %ld. Increase
activation/reserved_memory?
```

where **%ld** is replaced with the value of memory used. This provides better information about the source of the problem to the administrator. Preallocated memory can be changed in the **lvm.conf** file using the ***reserved_memory*** option.

BZ#773432

Due to an incorrect test condition in the underlying code, **lvm** operations could enter an infinite loop if the system contained 4 or more volume groups with duplicate names. With this update, the erroneous test condition has been corrected and **lvm** commands now complete as expected in this scenario.

Enhancements

BZ#575967

Some of the *lvm2* operations were optimized to speed up activation and deactivation time if running over a large group of logical volumes.

BZ#523324

The updated allocation policy now better handles allocation of new segments for mirrors with multiple segments (for example, mirrors which were repeatedly extended).

BZ#720971

The ext4 file system will now be automatically resized after executing the **lvextend** command with the **-r** option.

Users of *lvm2* should upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.102. lvm2-cluster

4.102.1. RHBA-2012:0223 — lvm2-cluster bug fix and enhancement update

An updated lvm2-cluster package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 5.

The lvm2-cluster package provides support for Logical Volume Management (LVM) in a clustered

environment.

The lvm2-cluster package has been upgraded to upstream version 2.02.88, which provides a number of bug fixes and enhancements over the previous version. The full list of changes is detailed in the WHATS_NEW file located in the /usr/share/doc/lvm2-[version]/ directory. This updated lvm2-cluster package ensures that the bug fixes provided with the lvm2 advisory for Red Hat Enterprise Linux 5 are also fixed in a clustered environment. (BZ#746687)

Enhancements

BZ#537369

This update adds the --nosync option to the lvextend command in the Clustered Logical Volume Manager (CLVM) mirrored volume extension.

BZ#638547

This update allows the clvm daemon to be restarted when volumes are in use.

All lvm2-cluster users are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.103. man-pages

4.103.1. RHBA-2011:1461 — man-pages bug fix and enhancement update

An updated man-pages package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 5.

The man-pages package provides man (manual) pages from the Linux Documentation Project (LDP).

Bug Fixes

BZ#699701

The host.conf(5) man page contained information about the "order" keyword, which is no longer used by the GNU C library, glibc, to determine the order in which host lookups are performed. The lookup order is now taken from /etc/nsswitch.conf. The unsupported keyword "order" has been removed from the host.conf man page.

BZ#698691

Previously, the rt_sigprocmask(2) manual page contained an erroneous description of the "oset" parameter. This update corrects this description.

BZ#640299

Previously, the db(3) manual page was pointing to the non-existent dbopen(3) manual page. An error message, "fopen: No such file or directory", was displayed when the command "man db" was issued. With this update, the db(3) manual page is removed.

BZ#751877

Previously, the tzset(3) manual page contained an incorrect interval in the description of the start and end format for Daylight Saving Time. Consequently users thought the number was 1-based rather than 0-based when not using the "J" option. With this update the manual page

has been corrected. The Julian day can be specified with an interval of 0 to 365 and February 29 is counted in leap years when the "J" option is not used.

Enhancements

BZ#650985

An update in the close(2) man page explains the interaction between system calls close() and recv() in different threads.

BZ#741713

The bootparam(7) man page is updated to the newer version.

All users are advised to upgrade to this updated man-pages package, which fixes these bugs and adds these enhancements.

4.104. man-pages-ja

4.104.1. RHBA-2011:1367 — man-pages-ja bug fix update

An updated man-pages-ja package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The man-pages-ja package contains Japanese translations of the Linux Documentation Project man pages.

Bug Fix

BZ#669002

Prior to this update, the Japanese translation of the iptables(8) man page contained a wrong description of the "--syn" option. The wrong description has been corrected in this update.

All users of man-pages-ja are advised to upgrade to this updated package, which fixes this bug.

4.105. man-pages-overrides

4.105.1. RHBA-2012:0259 — man-pages-overrides bug fix update

An updated man-pages-overrides package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The man-pages-overrides package contains a collection of manual (man) pages to complement other packages or update those contained therein.

Bug Fixes

BZ#510019

Previously, the Japanese version of the rpm(8) manual page contained multiple typos. This update corrects those typos.

BZ#647113

Previously, the manual page for the /usr/sbin/named_sdb binary was incorrectly named named-sdb(8). This update changes the name of the manual page to the correct named_sdb(8).

BZ#678326

Previously, the ethtool(8) manual page incorrectly referenced the "--blink" option in SYNOPSIS. The option has been modified to the correct "--identify" option.

BZ#703440

Previously, the dig(1) manual page did not document the exit codes of the dig tool. With this update, the exit codes are now described on the manual page.

BZ#766784

Previously, the lsvio(8) manual page did not document the "-D" and "-v" options. With this update, the options are now described on the manual page.

BZ#731938

Previously, multiple ecryptfs manual pages contained an incorrect link in the SEE ALSO section. With this update, the link is fixed.

BZ#769375

Previously, the man-pages-overrides package incorrectly overrode the mount.cifs(8) manual page from both the samba3x-client and samba-client packages. With this update, only the mount.cifs(8) manual page from the samba-client package is overridden.

BZ#749319

This update removes multiple manual pages from the original package.

All users of man-pages-overrides are advised to upgrade to this updated package, which fixes these bugs.

4.106. mesa

4.106.1. RHBA-2012:0288 — mesa bug fix update

Updated mesa packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

Mesa provides a 3D graphics API that is compatible with Open Graphics Library (OpenGL). It also provides hardware-accelerated drivers for many popular graphics chips.

Bug Fixes

BZ#442738

Under certain circumstances, when using Mesa's DRI driver for graphics with accelerated 3D support, the driver could incorrectly produce the following error message:

libGL warning: 3D driver claims to not support visual 0x5b

With this update, the error message no longer occurs.

BZ#508438

Mesa previously used a numerically unstable algorithm in an internal matrix inversion function, which caused the gluUnProject() and gluUnProject4() functions to return incorrect results. This update applies a patch based on upstream code that corrects the algorithm for matrix inversion used by Mesa. The gluUnProject() and gluUnProject4() functions now work as expected.

All users of mesa are advised to upgrade to these updated packages, which fix these bugs.

4.107. microcode_ctl

4.107.1. RHBA-2012:0189 — microcode_ctl bug fix and enhancement update

An updated microcode_ctl package that fixes two bugs and adds one enhancement is now available for Red Hat Enterprise Linux 5.

The microcode_ctl package provides microcode updates for Intel and AMD processors.

Bug Fixes

BZ#690414

A previous update introduced a memory leak when loading the updated microcode into memory before conversion of the microcode into a format suitable for the CPU. This update includes a corrected patch that de-allocates the memory correctly, ensuring memory does not leak.

BZ#760323

Previously, the command line definitions from the spec file specified an incorrect path (/etc/firmware/microcode.dat) to the microcode firmware. As a consequence, updating microcode_ctl failed with the following error message:

microcode_ctl: cannot open source file '/lib/firmware/microcode.dat'

This update modifies the firmware path to the correct /lib/firmware/microcode.dat, and microcode_ctl now updates correctly.

Enhancement

BZ#713653

The Intel CPU microcode file has been updated to version 20111110. This is the most recent version of the microcode available from Intel.

Note that the system must be rebooted in order for these changes to take effect.

All users of microcode_ctl are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.108. mkinitrd

4.108.1. RHBA-2011:1491 — mkinitrd bug fix update

Updated mkinitrd packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The mkinitrd utility creates file system images for use as initial RAM disk (initrd) images.

Bug Fix

BZ#753693

Due to an incomplete regular expression in the code, the mkinitrd utility did not recognize multipath devices located in the /dev/mpath/ directory. As a consequence, the system could not boot if such a multipath device contained the root file system. With this update, the regular expression has been corrected, and mkinitrd now correctly recognizes multipath devices in the /dev/mpath/ directory.

All users of mkinitrd are advised to upgrade to these updated packages, which fix this bug.

4.108.2. RHBA-2012:0157 — mkinitrd bug fix update

Updated *mkinitrd* packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

The *mkinitrd* utility creates the **initrd** file system image. The **initrd** image is an initial RAM disk that is loaded by a boot loader before the Linux kernel is started.

Bug Fixes

BZ#512892

Previously, due to missing code in the *mkinitrd* script, if two or more RAID arrays of the same level were created during installation, the **raid456.ko** module was loaded for every array of the same level. The system continued to boot but error messages for the second and subsequent arrays were displayed as follows:

```
insmod: error inserting '/lib/raid456.ko': -1 File exists
```

With this update the code has been improved and the *mkinitrd* script no longer attempts to load duplicate modules.

BZ#529158

Prior to this update, although the *mkinitrd* script included commands to setup a bonded connection, it did not configure the bonding mode first. Consequently, the bonded connection did not work and a host could not boot if the root partition on an iSCSI device was attached by a bonded channel. With this update, a patch has been applied to *mkinitrd* and hosts can now boot when their root partitions are on iSCSI devices attached by bonded connections.

BZ#532207

When probing for the root device, *mkinitrd* did not use the full device path for the root device when using **LABEL**-based mounts with *iSCSI RAID* arrays. Consequently, the following error message was logged when updating the kernel:

```
/sbin/scsi_id: option requires an argument -- s
```

With this update, a patch has been applied to *mkinitrd* and the error messages are no longer generated in the scenario described.

BZ#593096

Due to a regression, if the system's **lvm.conf** file had the ***command_names*** or **prefix** directives set, the output from **lvm.static** would be corrupted. With this update a patch has been applied to override the system settings while running *mkinitrd* and the **initrd** image created now has an uncorrupted **lvm.conf** file.

BZ#602409

Prior to this update, **nash**, the **linuxrc** image script interpreter, did not support the ***dirsync*** mount option for **ext3** file systems. Consequently, if the ***dirsync*** option was used for the root file system in the file systems table (**fstab**), the system did not boot. The following error message was logged:

```
EXT3-fs: Unrecognized mount option "dirsync" or missing value
```

This update includes a patch to support the ***dirsync*** option with the mount command and synchronous directory modifications can now be made while using **ext3** file systems.

BZ#620699

Due to a missing dependency, the *dmraid* package was not installed by default. Consequently, when running the *mkinitrd* command on IBM System/390 and IBM System z, the command failed and the following error message was displayed:

```
cp: cannot stat `/sbin/dmraid.static': No such file or directory
```

With this update, a requirement for *dmraid* has been added to the *mkinitrd* specification file (**mkinitrd.spec**). The **mkinitrd** command now works as expected on IBM System/390 and System z.

BZ#660731

Due to a regression in **libdhcp**, **netlink** interface flags were misinterpreted as standard interface flags by nash when it processed the **network** command. Consequently, the **DEBUG**, **PROMISC**, and **ALLMULTI** flags were incorrectly enabled on network interfaces. The problem has been corrected in **libdhcp** and the *mkinitrd* spec file has been changed to require *libdhcp-devel-1.20-12* or later. As a result, the incorrect flags are no longer set on the network interfaces.

BZ#679581

Prior to this update, the **grubby** command line tool for updating **bootloader** config files, terminated unexpectedly with a segmentation fault when the command **grubby --info=ALL** was executed and **grub.conf** contained Windows boot definitions. With this update, a patch has been applied and **grubby** no longer crashes but returns **non linux entry** in the scenario described.

BZ#696971

Previously, setting an attribute for all kernel entries in a config file using the **--update-kernel=ALL** command directive worked only once. Subsequent use of the **--update-kernel=ALL** command directive only updated the arguments for the first kernel entry found.

With this update a patch has been applied and the problem no longer occurs in the scenario described.

BZ#700102

The **mkinitrd** man page did not include **multipath** in its list of limitations for FIPS support. With this update, the man page entry for FIPS has been improved to say the following:

```
/boot  Must not be on multipath, nfs, dmraid or mdraid
```

BZ#700592

Prior to this update, after **/sbin/init** was executed the **nash-hotplug** process did not terminate itself and had to be terminated by a kill command in **/etc/rc.sysinit**. With this update, a patch has been applied to improve the code and **nash-hotplug** now exits when the parent process terminates.

BZ#744330

Due to an incomplete regular expression in the code, the **mkinitrd** utility did not recognize multipath devices located in the **/dev/mpath/** directory. As a consequence, the system could not boot if such a multipath device contained the root file system. With this update, the regular expression has been corrected, and *mkinitrd* now correctly recognizes multipath devices in the **/dev/mpath/** directory.

Users of *mkinitrd* should upgrade to these updated packages, which fix these bugs.

4.109. mod_auth_kerb

4.109.1. RHBA-2012:0057 — mod_auth_kerb bug fix update

An updated mod_auth_kerb package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The mod_auth_kerb package provides a module for the Apache HTTP Server designed to provide Kerberos authentication over HTTP. The module supports the Negotiate authentication method, which performs full Kerberos authentication based on ticket exchanges.

Bug Fix

BZ#783228

The mod_auth_kerb module did not use the Kerberos libraries in a thread-safe way. Therefore, if mod_auth_kerb ran under a multi-threaded Apache HTTP Server, authentication requests could terminate unexpectedly with a segmentation fault. With this update, the thread-safety problem has been fixed, and thread crashes no longer occur under these circumstances.

All users of mod_auth_kerb are advised to upgrade to this updated package, which fixes this bug.

4.110. mod_revocator

4.110.1. RHBA-2012:0247 — mod_revocator bug fix update

Updated mod_revocator packages that fix four bugs are now available for Red Hat Enterprise Linux 5.

The mod_revocator module retrieves and installs remote Certificate Revocation Lists (CRLs) into an Apache web server.

Bug Fixes

716355

Prior to this update, the mod_revoc module could not shut down the httpd server on 32-bit platforms and the error log infinitely reported the error message "service httpd status httpd (pid) when an expired CRL was downloaded. This update modifies mod_revocator so that the httpd server can correctly shut down and the error log now reports the error message "service httpd status httpd dead but subsys locked".

716361

Prior to this update, the mod_revoc module could not shut down the httpd server on 32-bit platforms when CRLUpdate failed. This update modifies mod_revocator so that the httpd server can correctly shut down when updating the CRL fails.

716874

Prior to this update, httpd failed to start if the 32-bit mod_revocator was installed on a 64-bit PowerPC platform. This update modifies the initialization size of the static array. Now, httpd servicestarts as expected.

737556

Prior to this update, CRLs could, under certain circumsatances, silently fail to be downloaded without any error message when the mod_revocator module was loaded successfully. This update resolves two segmentation violations. In addition, the setsebool -P httpd_can_network_connect=1 command can now be used to allow httpd to connect to a remote port which SELinux would otherwise deny when running mod_revocator. Now, CRLs are downloaded correctly when the mod_revocator module is running.

All users of mod_revocator are advised to upgrade to these updated packages, which fix these bugs.

4.111. mrtg

4.111.1. RHBA-2011:1493 — mrtg bug fix update

An updated mrtg package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network-links. MRTG generates HTML pages containing Portable Network Graphics (PNG) images, which provide a live, visual representation of this traffic.

Bug Fixes

BZ#436662

Previously, changing the "kMG" keyword in the MRTG configuration could cause the labels on the y-axis to overlap the main area of the generated chart. With this update, an upstream patch has been applied to address this issue, and changing the "kMG" keyword in the configuration no longer leads to the incorrect rendering of the resulting charts.

BZ#563619

Previously, the package incorrectly informed rpm/yum that it provides perl(SNMP_util), perl(SNMP_Session), perl(BER) and a few other capabilities. Because of that, rpm/yum preferred mrtg as a source for those capabilities over the real source (e.g. perl-SNMP_Session). This caused other packages that expect to receive perl-SNMP_Session to fail. This updated mrtg package does not state that it provides those capabilities and as a result rpm/yum will no longer incorrectly prefer it for those capabilities.

Users of mrtg should upgrade to this updated package, which resolves these issues.

4.112. mysql

4.112.1. RHSA-2012:0127 — Moderate: mysql security update

Updated mysql packages that fix several security issues are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

MySQL is a multi-user, multi-threaded SQL database server. It consists of the MySQL server daemon (mysqld) and many client programs and libraries.

Security Fixes

CVE-2012-0075, **CVE-2012-0087**, **CVE-2012-0101**, **CVE-2012-0102**, **CVE-2012-0114**, **CVE-2012-0484**, **CVE-2012-0490**

This update fixes several vulnerabilities in the MySQL database server. Information about these flaws can be found on the Oracle Critical Patch Update Advisory page:

http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

These updated packages upgrade MySQL to version 5.0.95. Refer to the MySQL release notes for a full list of changes:

http://dev.mysql.com/doc/refman/5.0/en/news-5-0-x.html

All MySQL users should upgrade to these updated packages, which correct these issues. After installing this update, the MySQL server daemon (mysqld) will be restarted automatically.

4.113. mysql-connector-odbc

4.113.1. RHEA-2012:0227 — mysql-connector-odbc bug fix update

An updated mysql-connector-odbc package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The mysql-connector-odbc package contains the Open Database Connectivity (ODBC) driver for MySQL.

BZ#743711

Previously, the mysql-connector-odbc package required the unixODBC package. However, this is not needed because the explicit dependency on the unixODBC shared library is sufficient. This update removes the dependency on the unixODBC package. As a result, the main unixODBC64 package can now be installed instead of unixODBC, and older ODBC applications can still use MySQL.

All users of mysql-connector-odbc are advised to upgrade to this updated package, which fixes this bug.

4.114. MySQL-python

4.114.1. RHBA-2012:0181 — MySQL-python bug fix update

An updated MySQL-python package that fixes multiple bugs is now available for Red Hat Enterprise Linux 5.

MySQL-python is an interface to the MySQL database server for Python.

The MySQL-python package has been upgraded to version 1.2.3c1, which provides multiple bug fixes over the previous version. (BZ#475854, BZ#555868)

Users who require MySQL-python are advised to upgrade to this updated package, which fixes these bugs.

4.115. net-snmp

4.115.1. RHBA-2011:1216 — net-snmp bug fix update

Updated net-snmp packages that fix a bug are now available for Red Hat Enterprise Linux 5.

SNMP (Simple Network Management Protocol) is a protocol used for network management. The NET-SNMP project includes various SNMP tools: an extensible agent, an SNMP library, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps and a version of the netstat command which uses SNMP. The net-snmp package contains the snmpd and snmptrapd daemons, documentation, etc.

Bug Fix

BZ#732943

In the previous net-snmp update, implementation of the UCD-SNMP-MIB::dskTable table was rewritten and reporting of the UCD-SNMP-MIB::dskPercentNode column was accidentally removed from the snmpd daemon. With this update, the object identifier for UCD-SNMP-MIB::dskPercentNode has been restored and it now properly reports percentages of used inodes on storage devices, thus fixing this bug.

All users of net-snmp are advised to upgrade to these updated packages, which fix this bug.

4.115.2. RHBA-2012:0165 — net-snmp bug fix update

Updated *net-snmp* packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

The *net-snmp* packages provide various libraries and tools for the Simple Network Management Protocol (SNMP), including an **SNMP** library, an extensible agent, tools for requesting or setting information from **SNMP** agents, tools for generating and handling **SNMP** traps, a version of the netstat command which uses **SNMP**, and a **Tk/Perl** Management Information Base (MIB) browser.

Bug Fixes

BZ#663789

Prior to this update, the SNMP daemon, **snmpd**, wrongly calculated CPU ticks on 32-bit platforms. This resulted in incorrect **UCD-SNMP-MIB::systemStats** being reported after more than 30 days of uptime. With this update, **snmpd** calculation of CPU ticks is fixed, and correct **systemStats** are now reported.

BZ#698562

Previously, **snmpd**, enumerated active TCP connections for **TCP-MIB::tcpConnectionTable** in a very inefficient way with O(n^2) complexity. With many TCP connections, an SNMP client could time out before **snmpd** processed a request regarding the **tcpConnectionTable,** and sent a response. This updated improves the enumeration mechanism and **snmpd** now swiftly responds to SNMP requests in the **tcpConnectionTable**.

BZ#706916

Prior to this update, the **snmpd** daemon did not properly recover when the system run out of memory when populating **IP-MIB::ipNetToPhysicalTable**. Consequently, the daemon sometimes terminated unexpectedly. This update adds additional checks to determine when running out of memory and the **snmpd** daemon no longer crashes in the scenario described.

BZ#714976

Prior to this update, **/usr/share/snmp/mibs/.index** was not marked in the *net-snmp* package specification file (spec file) as being exempt from verification. Consequently, the **rpm -V net-snmp**command sometimes reported a warning that file **/usr/share/snmp/mibs/.index** was modified. This file is updated by various SNMP applications and daemons, therefore it should not be checked by **rpm -V**. With this update, the **.index** file is explicitly marked as volatile and **rpm -V** no longer reports its updates.

BZ#716470

Prior to this update, the **Net-SNMP** tools and libraries did not support referencing an object in another file when parsing a *Management Information Base* (MIB) file and the error message Undefined NOTIFICATION was shown. With this update, references to objects are looked up in all referenced MIB files and thus **Net-SNMP** tools, including **snmptranslate**, no longer report errors when parsing such MIB files.

BZ#725339

In the previous **net-snmp** update, implementation of the **UCD-SNMP-MIB::dskTable** table was rewritten and reporting of the **UCD-SNMP-MIB::dskPercentNode** column was accidentally removed from the **snmpd** daemon. With this update, the object identifier for **UCD-SNMP-MIB::dskPercentNode** has been restored and it now properly reports percentages of used inodes on storage devices, thus fixing this bug.

BZ#725966

Prior to this update, **snmpd** could terminate unexpectedly when monitoring an *Object Identifier* (OID) using the ***monitor*** configuration option while the monitored OID was handled by the external AgentX subagent. With this update, a backported patch has been applied and the **snmpd** daemon no longer crashes when monitoring such OIDs.

BZ#736264

Prior to this update, when **snmpd** was started and did not find a network interface which was present during the last **snmpd** shutdown, the following error message was logged:

```
snmpd: error finding row index in _ifXTable_container_row_restore
```

This happened on systems which dynamically create and remove network interfaces on demand, such as virtual hosts or PPP servers. In this update, this message has been removed and no longer appears in the system log.

BZ#741789

In the previous *net-snmp* update, implementation of the **HOST-RESOURCES-MIB::hrStorageTable** table was rewritten and reporting of the **hrStorageUsed** column was wrongly calculated when the ***realStorageUnits*** config option was disabled. With this update, calculation of **hrStorageUsed** is fixed and is now reported correctly in **HOST-RESOURCES-MIB::hrStorageTable**.

BZ#743167

Prior to this update, the Net-SNMP perl module did not properly evaluate error codes in the **register()** method in the **NetSNMP::agent** module and terminated unexpectedly when this method failed. With this update, the **register()** method has been fixed and the updated perl modules no longer crash on failure.

BZ#744112

In the previous *net-snmp* update, the implementation of **HOST-RESOURCES-MIB::hrStorageTable** was rewritten and devices with Veritas File System (VxFS) were not reported. In this update, **snmpd** properly recognizes VxFS devices and reports them in **HOST-RESOURCES-MIB::hrStorageTable**.

BZ#748390

Prior to this update, AgentX subagents linked with **Net-SNMP** libraries did not properly check if an AgentX session was valid, or was already released, when sending a response through the session. This sometimes caused the subagent to terminate unexpectedly. In this update, all sessions are checked before a response is sent, thus the subagents no longer crash in the scenario described.

BZ#751235

Prior to this update, **snmpd** wrongly parsed the OID from the ***smuxpeer*** configuration option and thus rejected incoming **SMUX** communication. With this update, parsing of the ***smuxpeer*** configuration option is fixed and **snmpd** now accepts incoming **SMUX** requests as expected.

Users of *net-snmp* are advised to upgrade to these updated packages, which fix these bugs.

4.116. net-tools

4.116.1. RHBA-2012:0188 — net-tools bug fix update

An updated net-tools package that fixes multiple bugs is now available for Red Hat Enterprise Linux 5.

The net-tools package contains basic networking tools, including ifconfig, netstat, or route. Netstat, for example, prints information about the Linux networking subsystem.

Bug Fixes

BZ#319981

Previously, the "hostname -s" command returned the "hostname: Unknown host" error message on a host if a host name was not resolved in DNS (Domain Name System). The utility has been modified and now always returns a short host name instead of the error message.

BZ#531980

Previously, the mii-tool command displayed an I/O error on a network interface if the Intel e1000e driver was used. With this update, the tool is modified to only check generic Media Independent Interface (MII) registers defined in linux/mii.h. Now, the error message is no longer displayed.

BZ#622734

Previously, net-tools incorrectly used 32-bit integers for 64-bit architectures. As a result, certain entries in the "IpExt" section were displayed with negative values when running the "netstat -s" command. With this update, integers on 64-bit architectures are handled properly and the "netstat -s" command now produces the correct output.

BZ#668047

Prior to this update, the netstat utility could terminate unexpectedly with a stack smashing message when running the "netstat -nr -A inet6" command and /proc/net/ipv6_route contained lines of different length. With this update, the code that reads the content of /proc/net/ipv6_route is fixed and netstat no longer displays IpExt entries with negative values.

BZ#699698

Prior to this update, the route(8) manual page did not clearly describe that the "mss" option can set the maximum transmission unit (MTU) value. With this update, the route(8) manual page now includes a detailed description of the "mss" option.

BZ#707427

Prior to this update, the "netstat -p" command incorrectly displayed a number instead of the program name in the PID/Program name column. With this update, the code is modified and the command now correctly displays the program name.

BZ#707460

Prior to this update, several command line options were missing from the plipconfig(8) manual page. This update modifies the SYNOPSIS section and the usage output of the plipconfig

command to add these missing options.

BZ#732983

The netstat utility truncated IPv6 (Internet Protocol version 6) UDP sockets even if the "--notrim" or "-T" option was specified. With this update, complete IPv6 addresses are displayed for UDP sockets when using netstat with one of these options.

All users of net-tools are advised to upgrade to this updated package, which fixes these bugs.

4.117. netpbm

4.117.1. RHSA-2011:1811 — Important: netpbm security update

Updated netpbm packages that fix three security issues are now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The netpbm packages contain a library of functions which support programs for handling various graphics file formats, including .pbm (Portable Bit Map), .pgm (Portable Gray Map), .pnm (Portable Any Map), .ppm (Portable Pixel Map), and others.

Security Fixes

CVE-2011-4516, **CVE-2011-4517**

Two heap-based buffer overflow flaws were found in the embedded JasPer library, which is used to provide support for Part 1 of the JPEG 2000 image compression standard in the jpeg2ktopam and pamtojpeg2k tools. An attacker could create a malicious JPEG 2000 compressed image file that could cause jpeg2ktopam to crash or, potentially, execute arbitrary code with the privileges of the user running jpeg2ktopam. These flaws do not affect pamtojpeg2k.

CVE-2009-4274

A stack-based buffer overflow flaw was found in the way the xpmtoppm tool processed X PixMap (XPM) image files. An attacker could create a malicious XPM file that would cause xpmtoppm to crash or, potentially, execute arbitrary code with the privileges of the user running xpmtoppm.

Red Hat would like to thank Jonathan Foote of the CERT Coordination Center for reporting the CVE-2011-4516 and CVE-2011-4517 issues.

All users of netpbm are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

4.117.2. RHBA-2012:0287 — netpbm bug fix update

Updated netpbm packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The netpbm package contains a library of functions which support programs for handling various graphics file formats, including .pbm (portable bitmaps), .pgm (portable graymaps), .pnm (portable anymaps), .ppm (portable pixmaps) and others.

Bug Fixes

BZ#509366

Prior to this update, the pnmtofiasco and fiascotopnm utilities could not correctly read the bitfile on IBM System z and PowerPC platforms. As a consequence, images were not correctly converted. This update modifies pnmtofiasco so that the files are successfully converted.

BZ#510501

Prior to this update, the manual page for the pamperspective utility contained several misprints which could be confusing for users. This update corrects the misprints.

BZ#510759

Prior to this update, the pgmtopbm utility encountered problems when converting grayscale pgm images to black and white pbm images. As a consequence, the pgmtopbm utility generated an empty white image. This update modifies the conversion process so that the pbm image is displayed in black and white as expected.

BZ#574362

Prior to this update, the xwd image header contained incorrect information about the layout and the bit order when running on the rdesktop window. As a consequence, the xwdtopnm utility generated the wrong image colors. This update modifies the the xwd image header so that the correct output is displayed.

BZ#699633

Prior to this update, the manual pages for the pnmtojbig and pcdovtoppm utilities were missing. This update adds the missing documentation.

All users of netpbm are advised to upgrade to these updated packages, which fix these bugs.

4.118. nfs-utils

4.118.1. RHSA-2012:0310 — Low: nfs-utils security, bug fix, and enhancement update

An updated nfs-utils package that fixes one security issue, various bugs, and adds one enhancement is now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The nfs-utils package provides a daemon for the kernel Network File System (NFS) server, and related tools such as the mount.nfs, umount.nfs, and showmount programs.

Security Fix

CVE-2011-1749

It was found that the mount.nfs tool did not handle certain errors correctly when updating the mtab (mounted file systems table) file. A local attacker could use this flaw to corrupt the mtab file.

Bug Fixes

BZ#529588

The nfs service failed to start if the NFSv1, NFSv2, and NFSv4 support was disabled (the MOUNTD_NFS_V1="no", MOUNTD_NFS_V2="no" MOUNTD_NFS_V3="no" lines in /etc/sysconfig/nfs were uncommented) because the mountd daemon failed to handle the settings correctly. With this update, the underlying code has been modified and the nfs service starts successfully in the described scenario.

BZ#593097

When a user's Kerberos ticket expired, the "sh rpc.gssd" messages flooded the /var/log/messages file. With this update, the excessive logging has been suppressed.

BZ#600497

The crash simulation (SM_SIMU_CRASH) of the rpc.statd service had a vulnerability that could be detected by ISS (Internet Security Scanner). As a result, the rpc.statd service terminated unexpectedly with the following error after an ISS scan:

```
rpc.statd[xxxx]: recv_rply: can't decode RPC message!
rpc.statd[xxxx]: *** SIMULATING CRASH! ***
rpc.statd[xxxx]: unable to register (statd, 1, udp).
```

However, the rpc.statd service ignored SM_SIMU_CRASH. This update removes the simulation crash support from the service and the problem no longer occurs.

BZ#710020

The nfs-utils init scripts returned incorrect status codes in the following cases: if the rpcgssd and rpcsvcgssd daemon were not configured, were provided an unknown argument, their function call failed, if a program was no longer running and a /var/lock/subsys/$SERVICE file existed, if starting a service under an unprivileged user, if a program was no longer running and its pid file still existed in the /var/run/ directory. With this update, the correct codes are returned in these scenarios.

BZ#712438

The "nfsstat -m" command did not display NFSv4 mounts. With this update, the underlying code has been modified and the command returns the list of all mounts, including any NFSv4 mounts, as expected.

BZ#715523

Previously, the nfs manual pages described the fsc mount option; however, this option is not supported. This update removes the option description from the manual pages.

BZ#729603

The nfs-utils preinstall scriptlet failed to change the default group ID for the nfsnobody user to 65534. This update modifies the preinstall scriptlet and the default group ID is changed to 65534 after nfs-utils upgrade as expected.

BZ#736677

The mount.nfs command with the "-o retry" option did not try to mount for the time specified in the "retry=X" configuration option. This occurred due to incorrect error handling by the command. With this update, the underlying code has been fixed and the "-o retry" option works as expected.

Enhancement

BZ#513094

The noresvport option, which allows NFS clients to use insecure ports (ports above 1023), has been added to the NFS server configuration options.

All nfs-utils users are advised to upgrade to this updated package, which resolves these issues and adds this enhancement. After installing this update, the nfs service will be restarted automatically.

4.119. nfs-utils-lib

4.119.1. RHEA-2012:0299 — nfs-utils-lib enhancement update

An enhanced nfs-utils-lib package that adds one enhancement is now available for Red Hat Enterprise Linux 5.

The nfs-utils-lib package contains support libraries required by the programs in the nfs-utils package.

Enhancement

BZ#782153

Prior to this update, it was not possible to statically map usernames to NFSv4 file systems. This update adds the feature and the user can configure the static mapping in the /etc/idmapd.conf file.

All nfs-utils-lib users are advised to upgrade to this updated package, which adds this enhancement.

4.120. nfs4-acl-tools

4.120.1. RHBA-2012:0296 — nfs4-acl-tools bug fix update

An updated nfs4-acl-tools package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The nfs4-acl-tools package provides utilities for managing NFSv4 Access Control Lists (ACLs) on files and directories mounted on ACL-enabled NFSv4 file systems.

Bug Fix

BZ#693422

Due to a regression introduced in Red Hat Enterprise Linux 5.5, if the format of the input ACL file

was incorrect, the "nfs4_setfacl" command failed with the following unexpected message:

*** glibc detected *** nfs4_setfacl: double free or corruption (out)

This update applies a patch that corrects the memory handling process and the nfs4_setfacl command now fails with a useful error message if the input file syntax is invalid.

All users of nfs4-acl-tools are advised to upgrade to this updated package, which fixes this bug.

4.121. nss

4.121.1. RHSA-2011:1444 — Important: nss security update

Updated nss packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact.

Network Security Services (NSS) is a set of libraries designed to support the development of security-enabled client and server applications.

Security Fix

BZ#751366

It was found that the Malaysia-based Digicert Sdn. Bhd. subordinate Certificate Authority (CA) issued HTTPS certificates with weak keys. This update renders any HTTPS certificates signed by that CA as untrusted. This covers all uses of the certificates, including SSL, S/MIME, and code signing.

Note

Digicert Sdn. Bhd. is not the same company as found at digicert.com.

Note

This fix only applies to applications using the NSS Builtin Object Token. It does not render the certificates untrusted for applications that use the NSS library, but do not use the NSS Builtin Object Token.

This update also fixes the following bug on Red Hat Enterprise Linux 5:

Bug Fix

BZ#743508

When using mod_nss with the Apache HTTP Server, a bug in NSS on Red Hat Enterprise Linux 5 resulted in file descriptors leaking each time the Apache HTTP Server was restarted with the "service httpd reload" command. This could have prevented the Apache HTTP Server from functioning properly if all available file descriptors were consumed.

For Red Hat Enterprise Linux 6, these updated packages upgrade NSS to version 3.12.10. As well, they upgrade NSPR (Netscape Portable Runtime) to version 4.8.8 and nss-util to version 3.12.10 on Red Hat Enterprise Linux 6, as required by the NSS update. (BZ#735972, BZ#736272, BZ#735973)

All NSS users should upgrade to these updated packages, which correct this issue. After installing the update, applications using NSS must be restarted for the changes to take effect. In addition, on Red Hat Enterprise Linux 6, applications using NSPR and nss-util must also be restarted.

4.121.2. RHSA-2011:1282 — Important: nss and nspr security update

Updated nss and nspr packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having important security impact.

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications.

Netscape Portable Runtime (NSPR) provides platform independence for non-GUI operating system facilities.

Security Fix

BZ#734316

It was found that a Certificate Authority (CA) issued fraudulent HTTPS certificates. This update renders any HTTPS certificates signed by that CA as untrusted. This covers all uses of the certificates, including SSL, S/MIME, and code signing.

Note

This fix only applies to applications using the NSS Builtin Object Token. It does not render the certificates untrusted for applications that use the NSS library, but do not use the NSS Builtin Object Token.

These updated packages upgrade NSS to version 3.12.10 on Red Hat Enterprise Linux 4 and 5. As well, they upgrade NSPR to version 4.8.8 on Red Hat Enterprise Linux 4 and 5, as required by the NSS update. The packages for Red Hat Enterprise Linux 6 include a backported patch.

All NSS and NSPR users should upgrade to these updated packages, which correct this issue. After installing the update, applications using NSS and NSPR must be restarted for the changes to take effect.

4.121.3. RHBA-2012:0291 — nss and nspr bug fix update

Updated nss and nspr packages that fix three bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

The Network Security Services (NSS) libraries support the cross-platform development of security-enabled clients and server applications, the Netscape Portable Runtime (NSPR) provides platform independence for non-GUI operating system facilities.

Bug Fixes

BZ#348761

Prior to this update, the selinux policy for mod_nss did not allow for correct handling of access vector caches (AVC). As a consequence, AVC could fail when running NSS. This update modifies the selinux policy so that AVC is handled as expected.

BZ#704595

Prior to this update, the crmf library used a maximum length of 2048 bits for wrapped private keys. As a consequence, private keys exceeding the maximum lengths failed. With this update, the maximum key length is now identical with the the maximum modulus length.

BZ#713373

Prior to this update, certain file descriptors were not closed. As a consequence, a file descriptor leak resulted upon continued reloading of the httpd service. This update modifies the underlying code and the descriptors are now correctly closed.

All NSS and NSPR users are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.122. nss_ldap

4.122.1. RHBA-2011:1413 — nss_ldap bug fix update

An updated nss_ldap package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The nss_ldap package contains the nss_ldap and pam_ldap modules. The nss_ldap module is a plug-in which allows applications to retrieve information about users and groups from a directory server. The pam_ldap module allows a directory server to be used by PAM-aware applications to verify user passwords.

Bug Fix

BZ#743193

Previously, a fixed size buffer to store the LDAP configuration could exceed its size. As a consequence, nss_ldap failed when it was used with certain large configurations, especially on 64-bit architectures where pointers in internal data structures occupy twice as much space in the buffer as on 32-bit architectures. This caused situations where a certain LDAP configuration worked on 32-bit architecture but not on 64-bit architecture. With this update, the size of the buffer has been increased to 64 KB, and nss_ldap now works correctly with LDAP configurations that do not exceed the size of 64 KB.

All users of nss_ldap are advised to upgrade to this updated package, which fixes this bug.

4.122.2. RHBA-2012:0268 — nss_ldap bug fix and enhancement update

An enhanced nss_ldap package that fixes various bugs and provides an enhancement is now available for Red Hat Enterprise Linux 5.

The nss_ldap package contains the nss_ldap and pam_ldap modules. The nss_ldap module is a name service switch module which allows applications to retrieve information about users and groups from a directory server. The pam_ldap module allows a directory server to be used by PAM-aware applications

to verify user passwords.

Bug Fixes

BZ#593242

Previously, nss_ldap did not correctly handle the situation where "unreadable" files were present in the CA certificate directory. Consequently, nss_ldap failed when resolving usernames and groups while using TLS even if a valid readable certificate was available. This update corrects the problem and nss_ldap now ignores files that are not world readable and uses the readable certificate files as expected.

BZ#696707

In certain cases, nss_ldap failed to get a response from the Lightweight Directory Access Protocol (LDAP) server and the client became temporarily unable to query the server. This update applies a patch which improves the code and the server now responds as expected.

BZ#705841

The LDAP server stored its configuration in a fixed-size buffer that could have been exceeded with large configurations, thus causing nss_ldap to fail. This was especially likely to occur on 64-bit architectures where pointers to internal data structures occupy twice as much space in the buffer as on 32-bit architectures. This caused situations where a certain ldap configuration worked on 32-bit architecture but not on 64-bit architecture. With this update, the code has been modified to allow the use of larger ldap configurations without exceeding the buffer and nss_ldap now works correctly.

Enhancements

BZ#741419

Prior to this update, nss_ldap did not select the closest DNS records, but always selected the first record returned by DNS. This update changes the behavior to select the records based on the priority and weight fields.

All users of nss_ldap are advised to upgrade to this updated package, which fixes these bugs and provides this enhancement.

4.123. ntp

4.123.1. RHBA-2011:1454 — ntp bug fix update

An updated ntp package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The Network Time Protocol (NTP) is used to synchronize a computer's time with another referenced time source. This package includes the ntpd daemon which continuously adjusts system time and utilities used to query and configure the ntpd daemon.

Bug Fix

BZ#449750

The ntp-keygen utility always used the DES-CBC (Data Encryption Standard-Cipher Block Chaining) encryption algorithm to encrypt private NTP keys. This algorithm is not supported in

FIPS (Federal Information Processing Standard) mode. As a consequence, ntp-keygen generated empty private keys when it was used on systems with FIPS mode enabled. To solve this problem, a new "-C" option has been added for ntp-keygen that allows for selection of an encryption algorithm for private key files. Private NTP keys are now generated as expected on systems with FIPS mode enabled.

All users of ntp are advised to upgrade to this updated package, which fixes this bug.

4.124. oddjob

4.124.1. RHBA-2011:1492 — oddjob bug fix update

Updated oddjob packages which fix this bug are now available for Red Hat Enterprise Linux 5.

The oddjob service runs specified privileged tasks for unprivileged client applications which communicate with it through the system message bus.

Bug Fix

BZ#628683

Previously, the oddjob daemon closed shared connections when it was stopped. Consequently oddjob crashed when shutting down because it incorrectly attempted to close its default connection to the system message bus. With this update, oddjob allows the connection to be closed implicitly when the process exits, avoiding the crash.

All users of oddjob are advised to upgrade to these updated packages, which fixes this bug.

4.125. openais

4.125.1. RHBA-2011:1487 — openais bug fix update

An updated openais package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The Application Interface Specification (AIS) is an API and a set of policies for developing applications that maintain services during faults. The OpenAIS Standards Based Cluster Framework is an OSI-certified implementation of the Service Availability Forum AIS. The openais package contains the openais executable, OpenAIS service handlers, default configuration files and an init script.

Bug Fixes

BZ#752443

When stopping the cman service on a cluster node shutdown, the groupd daemon often exited with the "groupd: cpg_leave error retrying" error message, causing OpenAIS to become unresponsive. As a consequence, the cluster node was not shut down correctly. With this update, the underlying code has been modified to stop cman correctly. Cluster nodes can now be shut down as expected.

BZ#754717

Under certain circumstances, if the system clock was changed on a cluster node, cman could terminate unexpectedly on all cluster nodes, resulting in nodes not being fenced. As a

consequence, the cluster was not shut down gracefully and had to be rebooted manually. With this update, the underlying code has been modified to handle significant time changes. The cman service no longer terminates and the cluster no longer fails.

All users of openais are advised to upgrade to this updated package, which fixes these bugs.

4.125.2. RHBA-2011:1428 — openais bug fix update

An updated openais package that fixes three bugs is now available for Red Hat Enterprise Linux 5.

The Application Interface Specification (AIS) is an API and a set of policies for developing applications that maintain services during faults. The OpenAIS Standards Based Cluster Framework is an OSI-certified implementation of the Service Availability Forum AIS. The openais package contains the openais executable, OpenAIS service handlers, default configuration files and an init script.

Bug Fixes

BZ#731460

Previously, when OpenAIS was used in a lossy network, and a large number of configuration changes occurred, OpenAIS sometimes terminated unexpectedly. To solve this problem, the underlying source code has been modified, and OpenAIS no longer crashes in the scenario described.

BZ#739083

In rare cases, rapidly starting and stopping the openais service sometimes resulted in a deadlock. This update adapts the underlying source code to prevent such a deadlock, resolving this issue. Deadlock situations no longer happen during a rapid start/stop process.

BZ#739086

Under certain circumstances, the previous version of OpenAIS sometimes used an incorrect sort message queue when the "memb_join" message was sent during recovery. With this update, this error has been fixed, and OpenAIS now uses a correct sort message queue in this scenario.

All users of openais are advised to upgrade to this updated package, which fixes these bugs.

4.125.3. RHBA-2011:1262 — openais bug fix update

An updated openais package that fixes one bug is now available for Red Hat Enterprise Linux 5 Extended Update Support.

The Application Interface Specification (AIS) is an API and a set of policies for developing applications that maintain services during faults. The OpenAIS Standards Based Cluster Framework is an OSI-certified implementation of the Service Availability Forum AIS. This package contains the OpenAIS executable, OpenAIS service handlers, default configuration files and an init script.

Bug Fix

BZ#718773

Prior to this update, receive buffers could overflow and packets dropped under high traffic. As a result, the retransmit list appeared. This update processes incoming messages more frequently so there is no longer an overflow of receive buffers and dropping messages.

All OpenAIS users are advised to upgrade to this updated package, which fixes this bug.

4.125.4. RHBA-2012:0180 — openais bug fix and enhancement update

An updated openais package that fixes various bugs and adds one enhancement is now available for Red Hat Enterprise Linux 5.

The Application Interface Specification (AIS) is an API and a set of policies for developing applications that maintain services during faults. The OpenAIS Standards Based Cluster Framework is an OSI-certified implementation of the Service Availability Forum AIS. The openais package contains the openais executable, OpenAIS service handlers, default configuration files and an init script.

Bug Fixes

BZ#708335

Previously, the length of the array cpg_exec_service[]/cpg_exec_engine[] in OpenAIS and corosync differed. Consequently, OpenAIS failed if corosync ran on the same network. This update modifies the length of this array in OpenAIS. Now, OpenAIS and corosync successfully run on the same network.

BZ#718773

Previously, the receive buffers could overflow under heavy traffic. Consequently, packets could be lost and retransmit list error messages appeared in the log files. Now, incoming messages are processed more frequently, and the retransmit list error messages no longer appear.

BZ#726142

Previously, the OpenAIS service could, under certain circumstances, encounter a deadlock when starting or stopping the process. This update modifies the underlying source code to prevent such a deadlock. Deadlock situations no longer happen during a rapid start or stop process.

BZ#729081

Previously, OpenAIS could, under certain circumstances, terminate unexpectedly when OpenAIS was used in a network losing packets and a large number of configuration changes occurred. This update modifies the underlying source code, and OpenAIS no longer terminates under these circumstances.

BZ#734865

Previously, OpenAIS could, under certain circumstances, use an incorrect sort message queue when the "memb_join" message was sent during recovery. Consequently, OpenAIS could join all nodes. Now, OpenAIS uses the correct sort message queue if memb_join message is sent during recovery.

BZ#737100

Previously, openais_response_send could, under certain circumstances, change the value of req->ics_channel_handle. Consequently, OpenAIS terminated unexpectedly when using the subscribe function of the eventing (EVT) service. This update saves the handle outside the message. OpenAIS no longer terminates if an application is using the subscribe function of the EVT service.

BZ#738468

Previously, cman could, under certain circumstances, terminate unexpectedly on all cluster nodes and nodes were not fenced if the system clock was changed on a cluster node. Consequently, the cluster was not shut down gracefully and had to be rebooted manually. Now, the underlying code has been modified to handle significant time changes. The cman service no longer terminates and the cluster no longer fails.

BZ#746807

Previously, the groupd daemon often exited with the "groupd: cpg_leave error retrying" error message, causing OpenAIS to become unresponsive when stopping the cman service on a cluster node shutdown. Consequently, the cluster node was not shut down correctly. Now, the underlying code has been modified to stop cman correctly. Cluster nodes can be shut down as expected.

BZ#752952

Previously, totemip_parse used the getaddrinfo function without an associated freeaddrinfo call. Consequently, a small amount of memory leaked when calling OpenAIS. This update adds a call to freeaddrinfo. OpenAIS no longer leaks memory in totemip module.

Enhancement

BZ#703162

With this update, manual pages for ais-keygen, aisexec, openais-cfgtool and openais-confdb-display have been added to OpenAIS.

All users of openais are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.126. openCryptoki

4.126.1. RHBA-2012:0239 — openCryptoki bug fix update

An updated openCryptoki package that fixes four bugs is now available for Red Hat Enterprise Linux 5.

The openCryptoki package contains version 2.11 of the public-key cryptography standards (PKCS)#11 API, implemented for IBM Cryptocards. This package includes support for the IBM 4758 Cryptographic CoProcessor (with the PKCS#11 firmware loaded), the IBM eServer Cryptographic Accelerator (FC 4960 on IBM eServer System p), the IBM Crypto Express2 (FC 0863 or FC 0870 on IBM System z), and the IBM CP Assist for Cryptographic Function (FC 3863 on IBM System z).

Bug Fixes

BZ#538879

Prior to this update, the process to unwrap an Advanced Encryption Standard (AES) key could, under certain circumstances, fail after a hardware cryptographic token was initialized. As a result, openCryptoki returned the error "CKR_TEMPLATE_INCOMPLETE". This update modifies the AES key unwrapping process so that it no longer fails.

BZ#539168

Prior to this update, the message authentication code (MAC) could, under certain circumstances, fail to be verified when using the PKCS#11 API for the acceleration of cryptographic instructions and the error "411 = MAC did not verify." was retunred. This update modifies the underlying code so that the MAC is now computed successfully after being offloaded to the CPACF.

BZ#541028

Prior to this update, openCryptoki did not correctly recognize whether secure-key crypto support was installed when the pkcs11_startup and pkcs_slot scripts were running. As a consequence, the Common Cryptographic Architecture (CCA) token did not correctly work. This update modifies the pkcs11_startup and pkcs_slot scripts to improve the secure-key crypto support check. Now, the CCA token works as expected.

BZ#612274

Prior to this update, OpenCryptoki used linked lists to track objects and sessions in memory, performing an exhaustive search in practically every PKCS#11 call. As a consequence, the overall performance of cryptographic operations degraded exponentially with the number of objects per token or open sessions per process. This update modifies the underlying source code so that the overall performance remains constant.

All users of openCryptoki are advised to upgrade to these updated packages, which fix these bugs.

4.127. OpenIPMI

4.127.1. RHBA-2011:1107 — OpenIPMI bug fix update

Updated OpenIPMI packages that resolve an issue are now available for Red Hat Enterprise Linux 5.

The OpenIPMI packages provide command line tools and utilities to access platform information using IPMI (Intelligent Platform Management Interface), and thus allowing system administrators to manage systems and perform system health monitoring.

Bug Fix

BZ#722462

When IPMI-enabled devices reported SDR (sensor data record) records under a different owner than the BMC (Baseboard Management Controller), the IPMItool utility tried to retrieve these SDR records from the IPMI bus instead of the BMC bus. Due to timeout setting for the SDR read attempt, serious performance issues occurred and no sensor data was shown. This issue has been fixed and IPMItool now correctly reads these SDR records from the BMC and shows the correct sensor data on these platforms.

All users of OpenIPMI are advised to upgrade to these updated packages, which resolve this issue.

4.128. openldap

4.128.1. RHBA-2011:1482 — openldap bug fix update

Updated openldap packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The openldap packages contain configuration files, libraries, and documentation for OpenLDAP. OpenLDAP is an open source suite of Lightweight Directory Access Protocol (LDAP) applications and development tools. LDAP is a set of protocols for accessing directory services over the Internet, similar to the way Domain Name System (DNS) information is propagated over the Internet.

Bug Fix

BZ#750538

When running an OpenLDAP server with the LDAP Sync replication engine (syncrepl) enabled and a large amount of data was replicated, the memory was used extensively. Due to high memory usage, the standalone LDAP daemon (slapd) was sometimes not able to allocate enough free memory using its default memory allocation mechanism. As a consequence, slapd fell back on the secondary memory allocation mechanism but without freeing the memory properly, and thus causing memory leaks. With this update, the slpad daemon frees the memory correctly in such a scenario, and memory leaks no longer occur.

All users of openldap are advised to upgrade to these updated packages, which fix this bug.

4.128.2. RHEA-2011:1345 — openldap bug fix and enhancement update

Updated openldap packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 5.

OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. The openldap packages contain configuration files, libraries, and documentation for OpenLDAP.

Bug Fixes

BZ#734144

Prior to this update, some parts of OpenLDAP were impossible to debug due to incomplete debug data. The problem was caused by stripping debug data of some modules at an early stage of the package build process. This update disables the stripping and the openldap-debuginfo package is generated correctly.

BZ#734145

The openldap package compilation log contained information about breaking strict-aliasing rules. The presence of these warnings may have led into unexpected runtime behavior. The "-fno-strict-aliasing" option is now passed to a compiler to avoid optimizations that can produce invalid code. The change might contribute to stability and reliability of OpenLDAP.

Enhancement

BZ#733659

In a distributed environment, a Root DN (distinguished name) can be specified instead of a hostname to connect to an OpenLDAP server. The Root DN is used to look up the corresponding hosts using the DNS SRV (Domain Name Server Service) records. Prior to this update, the priority and weight of individual SRV records were ignored and the connection was created to the host in the first SRV record returned by the DNS server. As a consequence, a server in a different geographic location may have been queried, leading to high response

times. Servers are now queried according to their priority and weight, which conforms to the RFC 2782 standard.

Users are advised to upgrade to these updated openldap packages, which resolve these bugs and add this enhancement.

4.128.3. RHBA-2012:0155 — openldap bug fix and enhancement update

Updated *openldap* packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 5.

OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. LDAP is a set of protocols for accessing directory services (usually phone book style information, but other information is possible) over the Internet, similar to the way DNS (Domain Name System) information is propagated over the Internet. The *openldap* package contains configuration files, libraries, and documentation for OpenLDAP.

Bug Fixes

BZ#741184

When an OpenLDAP server was running with the LDAP Sync replication engine (**syncrepl**) enabled and a large amount of data was replicated, the memory was used extensively. Consequently, the standalone LDAP daemon (**slapd**) was sometimes not able to allocate enough free memory using its default memory allocation mechanism and **slapd** fell back on the secondary memory allocation mechanism without freeing the memory properly, causing memory leaks. With this update, the **slapd** daemon frees the memory correctly in such a scenario, and memory leaks no longer occur.

BZ#591419

Due to an error introduced in one of the previous updates, initializing a connection to a **slapd** server may have caused the CPU usage to reach 100% and the server to become unresponsive for about three seconds. With this update, an existing upstream patch has been applied to target this issue, and the OpenLDAP suite now works as expected.

BZ#641953

Previously, multiple concurrent connections to an OpenLDAP server could cause the **slapd** service to terminate unexpectedly with an assertion error. This update applies an upstream patch that adds mutexes to protect multiple threads from accessing a structure with a connection, and the slapd service no longer crashes.

BZ#655133

The **libldap** library did not provide the **ldap_init_fd()** function, even though certain utilities such as **cURL** rely on it and could not work properly as a result. This update applies a backported upstream patch that implements this API function, and these tools now work as expected.

BZ#620621

When the *openldap-servers* package was installed with the **syncrepl** utility configured, adding or removing data from a master server occasionally caused the **slapd** server to terminate

unexpectedly. An upstream patch has been provided and the crashes no longer occur in the described scenario.

BZ#665951

When running the **slapd** service with the **ppolicy** overlay enabled, an attempt to delete the **userPassword** attribute could cause the service to terminate unexpectedly, leaving the database in a corrupted state. With this update, an upstream patch has been applied to address this issue, and deleting the **userPassword** attribute no longer causes the **slapd** service to crash.

BZ#684630

Some parts of OpenLDAP were impossible to debug due to incomplete debug data. The problem was caused by stripping debug data of some modules at an early stage of the package build process. This update disables the stripping and the *openldap-debuginfo* package is generated correctly.

BZ#732381

Previously, the *openldap* package compilation log file contained warning messages returned by strict-aliasing rules. These warnings indicated that unexpected runtime behavior could occur. With this update, the **-fno-strict-aliasing** option is passed to the compiler to avoid optimizations that can produce invalid code, and no warning messages are now returned during package compilation.

BZ#609722

When the **openldap** client was configured with the **TLS_CACERTDIR** option, some of the certificate files were not accessible. Consequently, **openldap** could not establish TLS (Transport Layer Security) connections. An upstream patch has been provided to address this issue and **openldap** now establishes TLS connections to the server, even if some certificates specified in **TLS_CACERTDIR** are inaccessible.

BZ#738768

Previously, the **ldap** init script was incorrectly marked as a configuration file. When manual modifications had been made to it while the *openldap-servers* package was installed, and when the package had been updated, the init script was not overwritten as part of the upgrade. With this update, the *openldap* spec file has been updated to reflect that the **ldap** init script is not a configuration file, and *openldap-servers* now overwrites the init script properly in the described scenario.

BZ#604092

With the *openldap-servers* package was installed, when the server was shut down incorrectly and the database needed recovery, the **openldap** init script failed to start the server again. With this update, a new option has been added to the tool which checks **openldap** server configuration. The new option skips the database checks, and the **openldap** server now starts properly in the described scenario.

BZ#699652

The **ldap.conf(5)** manual page has been updated to emphasize that to specify Certificate

Authorities, the **TLS_CACERT** option is the preferred one to the **TLS_CACERTDIR** option.

BZ#563148

When the **migrate_all_offline.sh** script was used to migrate duplicate accounts, the migration process terminated. With this update, the script no longer interrupts the process, when certain errors occur. Local duplicate accounts no longer cause the migration process to interrupt.

Enhancement

BZ#733435

Previously, when a connection to an LDAP server was created by specifying search root DN (distinguished name) instead of the server hostname, the SRV records in DNS were requested and a list of LDAP server hostnames was generated. The servers were then queried in the order, in which the DNS server returned them but the priority and weight of the records were ignored. This update adds support for priority/weight of the DNS SRV records, and the servers are now queried according to their priority/weight, as required by RFC 2782.

All *openldap* users are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.129. openmotif

4.129.1. RHBA-2011:1451 — openmotif bug fix update

An updated openmotif package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The openmotif packages include the Motif shared libraries needed to run applications which are dynamically linked against Motif, as well as MWM, the Motif Window Manager.

Bug Fixes

BZ#583977

Prior to this update, the size set in the GeometryManager() function based on the XmFormConstraint "preferred_width" field was not updated when the label was changed and still contained the previous label length. Consequently, if the label text was modified while the window was smaller than the actual label width, the resulting size was incorrectly computed and the label text truncated. With this update the values are updated and the fault no longer occurs in the scenario described.

BZ#584287

Red Hat Enterprise Linux 6.0 was released with Open Motif 2.3.0, which introduced a bug in the LabelGadget widget. Consequently, under certain circumstances, LabelGadget could have drawn over a parent window with the background color and, if using the Xft fonts, also over the text. With this update, the text and background drawing the code has been corrected and the problem no longer occurs.

BZ#644824

Prior to this update, the XmeTraitSet() function in ToolTips added Traits but they were never

removed, even when the objects were destroyed, which resulted in memory leaks. With this update, the incorrect code has been fixed and memory leaks no longer occur in the scenario described.

BZ#684210

Prior to this update, the foreground and background color for insensitive labels (labels on items which are not currently sensitive or clickable) could sometimes be identical when using Xft fonts. As a consequence, text in insensitive labels using Xft fonts were invisible. With this update, the code has been corrected and the problem no longer occurs.

BZ#695650

Double free errors occur when free() is called more than once with the same memory address as an argument. Prior to this update, the helper widget "im_widget" could be closed twice, leading to a double free error, when the parent widget was closed. With this update, the code has been corrected and the problem no longer occurs.

All users of openmotif are advised to upgrade to this updated package, which fixes these bugs.

4.130. openscap

4.130.1. RHEA-2012:0209 — openscap bug fix and enhancement update

Updated openscap packages that fix various bugs and add several enhancements are now available for Red Hat Enterprise Linux 5.

The Security Content Automation Protocol (SCAP) is a line of standards that provide a standard language for the expression of Computer Network Defense (CND) related information. OpenSCAP is a set of open source libraries for the integration of SCAP.

The openscap packages have been upgraded to upstream version 0.8.0, which provides a number of bug fixes and enhancements over the previous version, including support for Open Vulnerability and Assessment Language (OVAL) version 5.8. (BZ#683579)

All users of openscap are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.131. openssh

4.131.1. RHBA-2011:1195 — openssh bug fix update

Updated openssh packages that resolve an issue are now available for Red Hat Enterprise Linux 5.

OpenSSH is OpenBSD's SSH (Secure Shell) protocol implementation. These packages include the core files necessary for both the OpenSSH client and server.

Bug Fix

BZ#730652

When Federal Information Processing Standards (FIPS) mode was enabled on a system, key-based authentication was always unsuccessful. This was caused by the newly introduced pubkey_key_verify() verification function, which did not take into consideration the fact that it

was running in a FIPS environment. With this update, the pubkey_key_verify() function has been modified to respect FIPS, and authentication using an RSA key is now successful without any issues when FIPS mode is enabled.

All users of openssh are advised to upgrade to these updated packages, which resolve this issue.

4.131.2. RHBA-2012:0237 — openssh bug fix and enhancement update

Updated openssh packages that fix multiple bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

OpenSSH is OpenBSD's Secure Shell (SSH) protocol implementation. These packages include the core files necessary for the OpenSSH client and server.

Bug Fixes

BZ#642935

Previously, the SSH daemon (sshd) attempted to bind port 22 to both Internet Protocol version 6 (IPv6) and Internet Protocol version 4 (IPv4). As a consequence, SSH targeted IPv4 and failed to bind after the second attempt. This update uses the IPV6_V6ONLY flag to allow SSH to listen to both on IPv4 and IPv6. (BZ#640857) * Previously, SELinux denied /sbin/setfiles access to a leaked SSH tcp_socket file descriptor when requested by the restorecon command. This update modifies sshd to set the file descriptors flag FD_CLOEXEC on the socket file descriptor. Now, sshd no longer leaks any descriptor.

BZ#674747

Previously, the pubkey_key_verify() function did not detect if it was running in a Federal Information Processing Standards (FIPS) environment. As a consequence, key-based authentication failed when the FIPS mode was enabled on a system. With this update, the pubkey_key_verify() function has been modified to respect FIPS. Now, authentication using an RSA key is successful when the FIPS mode is enabled.

BZ#681291

By default, OpenSSH used the /dev/urandom file to reseed the OpenSSL random number generator. Prior to this update, this random number generator was reseeded only once when the SSH daemon service, the SSH client, or an SSH-aware utility was started. To guarantee sufficient entropy, this update modifies the underlying source code to reseed the OpenSSL random number generator periodically. Additionally, the "SSH_USE_STRONG_RNG" environment variable has been added to allow users to specify /dev/random as the random number generator.

BZ#689406

Previously, the SELinux policy did not allow to execute the passwd command from sshd directly. With this update, sshd resets the default policy behavior before executing the passwd command.

BZ#706315

Previously, the lastlog command did not correctly report the last login log when processing users with User IDs (UIDs) greater than 2147483647. This update modifies the underlying code so that lastlog now works for all users.

BZ#710229

Previously, SSH did not send or accept the LANGUAGE environment variable. This update adds the SendEnv LANGUAGE option to the SSH configuration file and the AcceptEnv option to the sshd configuration file. Now, the environment variable LANGUAGE is send and received.

BZ#731925

Previously, running the mdoc option "groff -m" on OpenSSH manual pages caused formatting errors. This update modifies the manual page formatting. Now, the mdoc option "groff -m" runs as expected.

BZ#731930

Prior to this update, the ssh-copy-id script wrongly copied the identity.pub key instead of the id_rsa.pub key. This update modifies the underlying code so that ssh-copy-id now copies by default the id_rsa.pub key.

BZ#750725

Previously, SSH clients could, under certain circumstances, wait indefinitely at atomicio() in ssh_exchange_identification() when the SSH server stopped responding. This update uses the ConnectTimeout parameter to stop SSH clients from waiting after timeout.

Enhancement

BZ#720598

With this update the umask feature was added to the sftp subsystem to create a secure file transfer environment using the sftp service.

All users of openssh are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.132. openssl

4.132.1. RHSA-2012:0060 — Moderate: openssl security update

Updated openssl packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols, as well as a full-strength, general purpose cryptography library.

Security Fixes

CVE-2011-4108

It was discovered that the Datagram Transport Layer Security (DTLS) protocol implementation in OpenSSL leaked timing information when performing certain operations. A remote attacker

could possibly use this flaw to retrieve plain text from the encrypted packets by using a DTLS server as a padding oracle.

CVE-2011-4109

A double free flaw was discovered in the policy checking code in OpenSSL. A remote attacker could use this flaw to crash an application that uses OpenSSL by providing an X.509 certificate that has specially-crafted policy extension data.

CVE-2011-4576

An information leak flaw was found in the SSL 3.0 protocol implementation in OpenSSL. Incorrect initialization of SSL record padding bytes could cause an SSL client or server to send a limited amount of possibly sensitive data to its SSL peer via the encrypted connection.

CVE-2011-4619

It was discovered that OpenSSL did not limit the number of TLS/SSL handshake restarts required to support Server Gated Cryptography. A remote attacker could use this flaw to make a TLS/SSL server using OpenSSL consume an excessive amount of CPU by continuously restarting the handshake.

All OpenSSL users should upgrade to these updated packages, which contain backported patches to resolve these issues. For the update to take effect, all services linked to the OpenSSL library must be restarted, or the system rebooted.

4.132.2. RHBA-2012:0229 — openssl bug fix and enhancement update

Updated openssl packages that fix a bug and add various enhancements are now available for Red Hat Enterprise Linux 5.

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, as well as a full-strength general-purpose cryptography library.

Bug Fix

BZ#726593

Prior to this update, the openssl configuration file variables with "yes" or "no" values were parsed incorrectly. The value of "yes" was interpreted as "no". With this update, the "yes" or "no" values in the configuration file are now parsed correctly.

Enhancements

BZ#628976

Documentation of possible error states related to the FIPS mode is now included in the README.FIPS file.

BZ#735819

DigiCert Certification Authority certificates were added to the /etc/pki/tls/certs/ca-bundle.crt file that contains the certificates of trusted certification authorities.

BZ#740866

Known answer self-tests for the SHA2 algorithms (SHA256 and SHA512) were added to the FIPS mode start up self tests.

BZ#745410

The makefile for generating keys and certificates was updated to generate the private keys with a length of 2048 bits by default as the previous length of 1024 bits is now considered too weak.

All users of OpenSSL should upgrade to these updated packages, which fix this bug and add these enhancements.

4.133. openswan

4.133.1. RHSA-2011:1422 — Moderate: openswan security update

Updated openswan packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

Openswan is a free implementation of Internet Protocol Security (IPsec) and Internet Key Exchange (IKE). IPsec uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks.

Security Fix

CVE-2011-4073

A use-after-free flaw was found in the way Openswan's pluto IKE daemon used cryptographic helpers. A remote, authenticated attacker could send a specially-crafted IKE packet that would crash the pluto daemon. This issue only affected SMP (symmetric multiprocessing) systems that have the cryptographic helpers enabled. The helpers are disabled by default on Red Hat Enterprise Linux 5, but enabled by default on Red Hat Enterprise Linux 6.

Red Hat would like to thank the Openswan project for reporting this issue. Upstream acknowledges Petar Tsankov, Mohammad Torabi Dashti and David Basin of the information security group at ETH Zurich as the original reporters.

All users of openswan are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. After installing this update, the ipsec service will be restarted automatically.

4.133.2. RHBA-2012:0211 — openswan bug fix and enhancement update

Updated openswan packages that fix various bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

Openswan is a free implementation of Internet Protocol Security (IPsec) and Internet Key Exchange (IKE). IPsec uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks.

The openswan packages have been upgraded to upstream version 2.6.32, which provides a number of bug fixes and enhancements over the previous version. (BZ#698248)

Bug Fixes

BZ#549811

When an NSS database is created with a password (either in FIPS or non-FIPS mode), access to a private key (associated with a certificate or a raw public key) requires authentication. At authentication time, openswan passes the database password to NSS. Previously, when this happened, openswan also logged the password to /var/log/secure. The password could also be seen by running "ipsec barf". With this update, openswan still passes the database password at authentication time but no longer logs it in any fashion.

BZ#609343

The pluto key management daemon terminated unexpectedly with a segmentation fault when removing a logical IP interface. With this update the code has been improved, pluto now withdraws a connection to a dead logical interface cleanly and no longer crashes in the scenario described.

BZ#652733

Due to an error in a buffer initialization, the following message may have been written to the /var/log/secure log file during the IKE negotiation: "size ([size]) differs from size specified in ISAKMP HDR ([size])". Consequently, the establishment of secure connections could be significantly delayed. This update applies an upstream patch that resolves this issue, and the establishment of IPsec connections is no longer delayed.

Enhancements

BZ#524191

With this update, the openswan packages now include support for message digest algorithm HMAC-SHA1-96 as per RFC 2404.

BZ#591104

RFC 5114, Additional Diffie-Hellman Groups for Use with IETF Standards, adds eight Diffie-Hellman groups (three prime modulus groups and five elliptic curve groups) to the extant 21 groups set out in previous RFCs (e.g. RFCs 2409, 3526 and 4492) for use with IKE, TLS, SSH and so on.

This update implements groups 22, 23 and 24: a 1024-bit MODular exPonential (MODP) Group with 160-bit Prime Order Subgroup; a 2048-bit MODP Group with 224-bit Prime Order Subgroup; and a 2048-bit MODP Group with 256-bit Prime Order Subgroup respectively.

Note

Implementation of group 24 (a 2048-bit MODP Group with 256-bit Prime Order Subgroup) is required for US National Institute of Standards and Technology (NIST) IPv6 compliance and ongoing FIPS-140 certification.

All users of openswan are advised to upgrade to these updated packages, which fix these bugs and provide these enhancements.

4.134. oprofile

4.134.1. RHEA-2012:0267 — oprofile enhancement update

Updated oprofile packages that add two enhancements are now available for Red Hat Enterprise Linux 5.

OProfile is a system-wide profiler for Linux systems. The profiling runs transparently in the background and profile data can be collected at any time. OProfile uses the hardware performance counters provided on many processors, and can use the Real Time Clock (RTC) for profiling on processors without counters.

Enhancements

BZ#713667

Previously, the OProfile profiler did not provide the performance monitoring events for the Intel Core i3, i5, i7 and other processors formerly code named "Sandy Bridge". This update provides the files specific to the performance events of processors formerly code named "Sandy Bridge" and adds support for identification of these processors.

BZ#643476

Previously, the OProfile profiler did not identify the processors based on the Intel Xeon Processor E56XX, L56XX, W36XX and X56XX families. As a result, OProfile used the fallback Intel Architected events. With this update, OProfile provides the events specific to the processors based on the Intel Xeon Processor E56XX, L56XX, W36XX and X56XX families.

All OProfile users are advised to upgrade to these updated packages, which add these enhancements.

4.135. pam_krb5

4.135.1. RHBA-2012:0246 — pam_krb5 bug fix update

An updated pam_krb5 package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The pam_krb5 package allows PAM-aware applications to check user passwords with the help of a Kerberos KDC.

Bug Fix

BZ#715073

Previously, if a system was configured to perform Kerberos authentication using PKINIT, users who attempted to change their passwords using the "passwd" command or other PAM-aware application, while a smart card was inserted, would be erroneously prompted for the smart card PIN. With this update, the plugin returns an error to any requests for non-password information while attempting to obtain password-changing credentials. As a result, the unnecessary request for the smart card PIN is no longer made to the user in the scenario described.

All users of pam_krb5 are advised to upgrade to this updated package, which fixes this bug.

4.136. pam_pkcs11

4.136.1. RHBA-2012:0215 — pam_pkcs11 bug fix update

An updated pam_pkcs11 package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The pam_pkcs11 package allows X.509 certificate-based user authentication. It provides access to the certificate and its dedicated private key with an appropriate Public Key Cryptographic Standards #11 (PKCS#11) module.

Bug Fix

BZ#623640

The commands "pklogin_finder" and "pkcs11_inspect", both call "pk_configure" with their entire "argv" array. This includes the command name, which is not recognized as a valid option. Consequently, when running pklogin_finder or pkcs11_inspect, unnecessary error messages were written to the system log in the following format:

pkcs11_inspect: argument /usr/bin/pkcs11_inspect is not supported by this module This update applies a patch that improves the code, and the unnecessary error messages are no longer generated.

All users of pam_pkcs11 are advised to upgrade to this updated package, which fixes this bug.

4.137. pango

4.137.1. RHSA-2011:1326 — Moderate: pango security update

Updated pango packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

Pango is a library used for the layout and rendering of internationalized text.

Security Fix

CVE-2011-3193

A buffer overflow flaw was found in HarfBuzz, an OpenType text shaping engine used in Pango. If a user loaded a specially-crafted font file with an application that uses Pango, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

Users of pango are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, you must restart your system or restart the X server for the update to take effect.

4.138. parted

4.138.1. RHBA-2012:0192 — parted bug fix update

An updated parted package that fixes several bugs is now available for Red Hat Enterprise Linux 5.

The GNU Parted program allows creating, destructing, resizing, moving, and copying of hard disk partitions. Parted can be used to create space for new operating systems, reorganizing disk usage, and copying data to new hard disks.

Bug Fixes

BZ#582907

Prior to this update, the parted utility did not handle the return value of the dm_task_run() call correctly on device-mapper devices. As a consequence, parted returned a 0 exit status even if an error occurred. The utility has been modified and now correctly returns 1 if an error occurs.

BZ#584057

The mkpartfs command did not correctly handle partitions greater than 2 terabytes (TB) due to truncation of calculated block addresses. As a consequence, mkpartfs terminated with an error message. With this update, mkpartfs can now handle partitions greater than 2TB correctly.

BZ#623268

Prior to this update, parted incorrectly calculated the position of a new partition if the size of the partition was 1 or smaller (for example 1GB, 0.5GB). This was due to the snap_to_boundaries() function which rounded the endpoint of the partition down. As a result, an extremely small partition was created. The source code has been modified and defining units smaller than 1 is no longer allowed. The next smaller units should be used; for example, 500MB instead of 0.5GB. The 0 value is still allowed when specifying the start of the device.

BZ#675650

Previously, parted did not recognize more than 128 block devices. As a consequence, the model item displayed "Unknown". This update adds support for devices with major numbers in the range of 128 to 135 and the model name is now displayed correctly.

All users of parted are advised to upgrade to this updated package, which fixes these bugs.

4.139. pciutils

4.139.1. RHBA-2012:0251 — pciutils bug fix and enhancement update

Updated pciutils packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 5.

The pciutils packages provide various utilities for inspecting and manipulating devices connected to the Peripheral Component Interconnect (PCI) bus.

Bug Fix

BZ#684131

Prior to this update, the pciutils directory daemon did not call closedir(). As a consequence, the

directory could not be closed. This update modifies the underlying source code so that the directory is now closed after processing.

Enhancements

BZ#662556, BZ#759744

With this update, TPH (Transaction Processing Hints) and LTR (Latency Tolerance Reporting) reporting capabilities have been added to the pciutils package to support the PCI Express 3.0 standard.

All pciutils users are advised to upgrade to these updated packages, which fix this bug and add this enhancement.

4.140. pdksh

4.140.1. RHBA-2011:1394 — pdksh bug fix update

An updated pdksh package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The pdksh package contains a public domain implementation the Korn shell (ksh-88). The ksh shell is a command interpreter intended for both interactive and shell script use.

Bug Fix

634666

Prior to this update, when a SIGINT or SIGTERM was sent to a pdksh process, the signal was propagated to the entire process group. As a consequence sending SIGTERM to a process killed other processes even if the first process was not the parent. With this update the SIGINT and SIGTERM signals are correctly propagated and unexpected termination of processes no longer occurs.

All users of pdksh are advised to upgrade to this updated package, which fixes this bug.

4.141. perl

4.141.1. RHSA-2011:1797 — Moderate: perl security update

Updated perl packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Perl is a high-level programming language commonly used for system administration utilities and web programming.

Security Fixes

CVE-2011-3597

It was found that the "new" constructor of the Digest module used its argument as part of the string expression passed to the eval() function. An attacker could possibly use this flaw to execute arbitrary Perl code with the privileges of a Perl program that uses untrusted input as an argument to the constructor.

CVE-2010-2761

It was found that the Perl CGI module used a hard-coded value for the MIME boundary string in multipart/x-mixed-replace content. A remote attacker could possibly use this flaw to conduct an HTTP response splitting attack via a specially-crafted HTTP request.

CVE-2010-4410

A CRLF injection flaw was found in the way the Perl CGI module processed a sequence of non-whitespace preceded by newline characters in the header. A remote attacker could use this flaw to conduct an HTTP response splitting attack via a specially-crafted sequence of characters provided to the CGI module.

All Perl users should upgrade to these updated packages, which contain backported patches to correct these issues. All running Perl programs must be restarted for this update to take effect.

4.141.2. RHBA-2012:0199 — perl bug fix update

Updated perl packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

Perl is a high-level programming language commonly used for system administration utilities and web programming.

Bug Fixes

BZ#548249

Due to an error in the threads module, memory was leaked each time a thread was detached. Over time, this could cause long-running threaded Perl programs to consume a significant amount of memory. With this update, a patch has been applied to ensure the allocated memory is properly freed when a thread is detached, and using threads in Perl applications no longer causes memory leaks.

BZ#523827

If the "-default" parameter contained a plus sign ("+"), the CGI::popup_menu() method failed to generate valid HTML code and the closing tag of a paired tag was sometimes missing. The regular expression that contributes the HTML code in such scenarios has been fixed and the closing tag is now always present.

BZ#537777

Previously, joining or undefining a thread variable in a Perl script resulted in the following error message: "Attempt to free unreferenced scalar: SV 0x7b7dcb0, Perl interpreter: 0x7b4cfb0 during global destruction." A backported upstream patch has been provided and the internal error is no longer returned in the described scenario.

BZ#590644

Previously, the CGI::popup_menu() method generated invalid HTML code; a space character was sometimes missing between two attributes of a tag. With this update, the regular

expression responsible for generating such code has been fixed and the space characters are now properly generated in the described scenario.

BZ#675863

When threads were being rapidly created and detached on a multi-processor system with Perl, a variety of unexpected terminations occurred as a result. With this update, the threads module has been updated to version 1.79 and the crashes no longer occur.

BZ#593752

Previously, the NDBM_File module was missing in Perl packages and Perl could not provide support for NDBM files. With this update, NDBM_File has been added back to the Perl RPM packages.

BZ#676050

Previously, string evaluation in Perl threads sometimes resulted in an unexpected termination of the process. To partially fix this bug, handling of these strings has been moved to non-threaded variables. The update of the threads module to version 1.79 also contributed to the fix of this bug. Now, the crashes no longer occur in the described scenario.

BZ#621542

Due to a missing definition in Unicode table 4.0, Perl did not recognize the small letter Palochka (U+04cf). With this update, the Unicode table has been updated to version 5.0.1 and Palochka letters are now supported in Perl.

BZ#625746

When two nested loops were using the same iterator, the interpreter tried to double-free the iterator, resulting in a warning. Moreover, referring such an iterator caused the "Attempt to free unreferenced scalar" run-time error message to be returned. A backported patch from Perl 5.10.1 has been applied to handle shared iterators properly and no warnings or error messages are now returned in the described scenario.

BZ#676547

Previously, the value of a variable used for string evaluation was too small. Consequently, a large number of string evaluations made the interpreter return syntax error messages. Now, the variable for storing strings is using a bigger value and the error messages are no longer returned in the described scenario.

Users of perl are advised to upgrade to these updated packages, which fix these bugs.

4.142. perl-XML-SAX

4.142.1. RHBA-2011:1446 — perl-XML-SAX bug fix update

An updated perl-XML-SAX package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

XML::SAX is a SAX parser access API for Perl. It includes classes and APIs required for implementing

SAX drivers, along with a factory class for returning any SAX parser installed on the user's system.

Bug Fixes

BZ#641735

Parsing a long XML document with the XML::Simple API took an unacceptably long time if the XML::SAX parser implementation was available. The XML::SAX parser implementation was not optimized for large string variables (e.g. 2 MB). The XML::SAX parser has been updated to handle the reading of large strings in a more efficient way. This update enables long XML documents to be parsed in a more reasonable time.

BZ#744200

XML documents which have a whitespace character as the first character were not handled correctly. A warning, "Unable to recognize encoding of this document", was printed. With this update, encoding detection code has been changed to recognize XML documents with leading whitespace as a document without an XML declaration and with a default encoding. The warning is no longer printed as such documents are valid documents with encoding detection rules conforming to documents without an XML declaration.

All users of perl-XML-SAX are advised to upgrade to this updated package, which resolves these bugs.

4.143. php

4.143.1. RHSA-2012:0093 — Critical: php security update

Updated php packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fix

CVE-2012-0830

It was discovered that the fix for CVE-2011-4885 (released via RHSA-2012:0071, RHSA-2012:0033, and RHSA-2012:0019 for php packages in Red Hat Enterprise Linux 4, 5, and 6 respectively) introduced an uninitialized memory use flaw. A remote attacker could send a specially-crafted HTTP request to cause the PHP interpreter to crash or, possibly, execute arbitrary code.

All php users should upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

4.143.2. RHBA-2012:0249 — php bug fix and enhancement update

Updated php packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Bug Fixes

BZ#548142

PNG files in certain formats, which were loaded with the "gd" extension, were displayed incorrectly. This update adds support for such files and the files are now loaded correctly.

BZ#552436

Connecting to an Internet Message Access Protocol (IMAP) service could fail with the following error message:

PHP Warning: imap_open(): Couldn't open stream

This happened if the server advertised support for Kerberos authentication, but the client was not configured to use Kerberos. This update adds the DISABLE_AUTHENTICATOR option for the imap_open() function, which allows to disable a specific authentication method.

BZ#594813

A PHP script that is using the ODBC interfaces could enter a deadlock if the maximum execution time period expires while it is executing an SQL statement. This occurs because the execution timer uses a signal and the invoked ODBC functions are not reentrant. This update modifies the underlying code so the deadlock is less likely to occur.

BZ#607453

Previously, the PHP mktime() function and some daytime functions were limited to 32-bit time stamps on 64-bit platforms due to a build configuration error. This update fixes the error and allows the use of 64-bit time stamps on 64-bit platforms.

BZ#611662

If a prepared statement was unset when using PostgreSQL through the PHP Data Objects (PDO) interface, the current transaction was aborted. This caused subsequent SQL queries in the transaction to fail. With this update, the prepared statement is unset correctly and subsequent queries work as expected.

BZ#695251

If a negative array index value was sent to the var_export() function, the function returned an unsigned index ID. With this update, the function has been modified to process negative array index values correctly.

Enhancement

BZ#572359

The php package description has been improved.

All php users are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.144. php53

4.144.1. RHSA-2012:0092 — Critical: php53 security update

Updated php53 packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fix

CVE-2012-0830

It was discovered that the fix for CVE-2011-4885 (released via RHSA-2012:0019 for php53 packages in Red Hat Enterprise Linux 5) introduced an uninitialized memory use flaw. A remote attacker could send a specially- crafted HTTP request to cause the PHP interpreter to crash or, possibly, execute arbitrary code.

All php53 users should upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

4.144.2. RHSA-2011:1423 — Moderate: php53 and php security update

Updated php53 and php packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 respectively.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

CVE-2011-2483

A signedness issue was found in the way the PHP crypt() function handled 8-bit characters in passwords when using Blowfish hashing. Up to three characters immediately preceding a non-ASCII character (one with the high bit set) had no effect on the hash result, thus shortening the effective password length. This made brute-force guessing more efficient as several different passwords were hashed to the same value.

Note

Due to the CVE-2011-2483 fix, after installing this update some users may not be able to log in to PHP applications that hash passwords with Blowfish using the PHP crypt() function. Refer to the upstream "CRYPT_BLOWFISH security fix details" document, linked to in the References, for details.

CVE-2011-0708

An insufficient input validation flaw, leading to a buffer over-read, was found in the PHP exif

extension. A specially-crafted image file could cause the PHP interpreter to crash when a PHP script tries to extract Exchangeable image file format (Exif) metadata from the image file.

CVE-2011-1466

An integer overflow flaw was found in the PHP calendar extension. A remote attacker able to make a PHP script call SdnToJulian() with a large value could cause the PHP interpreter to crash.

CVE-2011-1468

Multiple memory leak flaws were found in the PHP OpenSSL extension. A remote attacker able to make a PHP script use openssl_encrypt() or openssl_decrypt() repeatedly could cause the PHP interpreter to use an excessive amount of memory.

CVE-2011-1148

A use-after-free flaw was found in the PHP substr_replace() function. If a PHP script used the same variable as multiple function arguments, a remote attacker could possibly use this to crash the PHP interpreter or, possibly, execute arbitrary code.

CVE-2011-1469

A bug in the PHP Streams component caused the PHP interpreter to crash if an FTP wrapper connection was made through an HTTP proxy. A remote attacker could possibly trigger this issue if a PHP script accepted an untrusted URL to connect to.

CVE-2011-1471

An integer signedness issue was found in the PHP zip extension. An attacker could use a specially-crafted ZIP archive to cause the PHP interpreter to use an excessive amount of CPU time until the script execution time limit is reached.

CVE-2011-1938

A stack-based buffer overflow flaw was found in the way the PHP socket extension handled long AF_UNIX socket addresses. An attacker able to make a PHP script connect to a long AF_UNIX socket address could use this flaw to crash the PHP interpreter.

CVE-2011-2202

An off-by-one flaw was found in PHP. If an attacker uploaded a file with a specially-crafted file name it could cause a PHP script to attempt to write a file to the root (/) directory. By default, PHP runs as the "apache" user, preventing it from writing to the root directory.

All php53 and php users should upgrade to these updated packages, which contain backported patches to resolve these issues. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

4.144.3. RHBA-2012:0266 — php53 bug fix update

Updated php53 packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

PHP is an HTML-embedded scripting language commonly used with Apache HTTP Server.

Bug Fixes

BZ#700724

If a negative array index value was sent to the var_export() function, the function returned an unsigned index ID. With this update, the function has been modified to process negative array index values correctly.

BZ#717158

Previously, subpackages of the php53 package did not contain the "Provides" definition corresponding to the definitions of the php package. This update adds the missing "Provides" definitions for these subpackages.

All users of php53 are advised to upgrade to these updated packages, which contain backported patches that fix these bugs. The httpd daemon must be restarted in order for these changes to take effect.

4.145. piranha

4.145.1. RHBA-2012:0262 — piranha bug fix update

An updated piranha package that fixes two bugs and adds one enhancement is now available for Red Hat Enterprise Linux 5.

Piranha provides high-availability and load balancing services for Red Hat Enterprise Linux. The piranha package contains various tools to administer and configure the Linux Virtual Server (LVS), as well as the heartbeat and failover components. LVS is a dynamically-adjusted kernel routing mechanism that provides load balancing, primarily for Web and FTP servers.

Bug Fixes

BZ#708035

Previously, the piranha-gui utility reported an HTTP 414 error (Request-URI Too Long) if too many virtual servers were defined. As a consequence, when trying to edit a virtual server, the "Too many arguments in the URL" error message appeared. With this update, the number of defined virtual servers does not affect the length of the URI and error messages are no longer reported.

BZ#725367

Previously, the pulse service did not correctly stop the ipvsadm sync daemon due to incorrect ipvsadm syntax. As a consequence, multiple sync daemons existed after restarting the pulse. With this update, the correct syntax is used. The pulse service now stops all the sync daemons, and exactly one master sync daemon and one backup sync daemon exist at any given time.

Enhancement

BZ#698505

This update adds the 255.255.254.0 network mask to the piranha-gui drop-down menus.

All users of piranha are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.146. poppler

4.146.1. RHBA-2012:0236 — poppler bug fix update

Updated poppler packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

Poppler is a Portable Document Format (PDF) rendering library used by applications such as Evince.

Bug Fixes

BZ#467285

When working with a PDF document with text spanning multiple columns, text selection may not have followed the flow of the text. This update improves the text selection to respect the text flow.

BZ#501716

A regression was introduced in the previous security update, RHSA-2009:0480, that prevented poppler from rendering PDFs which contained arithmetically encoded JBIG2 images with an unknown length. Specifically, poppler was unable to render PDFs generated by a Xerox WorkCentre 7232 scanner. With this update, such PDFs render correctly, as expected.

BZ#525311

Previously, poppler was unable to open some PDF files created with Adobe Acrobat due to incorrect determination of the position in the JBIG2 stream. With this update, such PDFs open correctly.

BZ#598945

Due to an error in memory allocation, previous versions of poppler may have terminated unexpectedly while rendering certain PDF documents. With this update, the underlying source code has been modified to address this issue, and poppler no longer fails to render such PDF documents.

BZ#637124

Previously, poppler was unable to open some PDF files due to unsupported security feature and the file opening failed with the following error:

Error: Unsupported version/revision (4/4) of Standard security handler Error: Incorrect password With this update, the underlying source code has been modified and such PDF files open as expected.

BZ#698052

Prior to this update, certain PDF documents may have been rendered with some characters displayed backwards. With this update, an upstream patch has been applied to ensure that poppler takes into account the horizontal scaling when updating the font, and such PDF documents are now rendered correctly.

All users of poppler are advised to upgrade to these updated packages, which fix these bugs.

4.147. postgresql

4.147.1. RHSA-2011:1377 — Moderate: postgresql security update

Updated postgresql packages that fix one security issue are now available for Red Hat Enterprise Linux 4, 5, and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

PostgreSQL is an advanced object-relational database management system (DBMS).

Security Fix

CVE-2011-2483

A signedness issue was found in the way the crypt() function in the PostgreSQL pgcrypto module handled 8-bit characters in passwords when using Blowfish hashing. Up to three characters immediately preceding a non-ASCII character (one with the high bit set) had no effect on the hash result, thus shortening the effective password length. This made brute-force guessing more efficient as several different passwords were hashed to the same value.

Note

Due to the CVE-2011-2483 fix, after installing this update some users may not be able to log in to applications that store user passwords, hashed with Blowfish using the PostgreSQL crypt() function, in a back-end PostgreSQL database. Unsafe processing can be re-enabled for specific passwords (allowing affected users to log in) by changing their hash prefix to "$2x$".

For Red Hat Enterprise Linux 6, the updated postgresql packages upgrade PostgreSQL to version 8.4.9. Refer to the PostgreSQL Release Notes for a full list of changes:

http://www.postgresql.org/docs/8.4/static/release.html

For Red Hat Enterprise Linux 4 and 5, the updated postgresql packages contain a backported patch.

All PostgreSQL users are advised to upgrade to these updated packages, which correct this issue. If the postgresql service is running, it will be automatically restarted after installing this update.

4.147.2. RHBA-2011:1447 — postgresql bug fix update

Updated postgresql packages that fix one bug are now available for Red Hat Enterprise Linux 5.

PostgreSQL is an advanced Object-Relational database management system (DBMS). The base postgresql package includes client programs and libraries that are needed to access a PostgreSQL DBMS server.

Bug Fix

BZ#728828

The client library for PostgreSQL, libpq, sets up OpenSSL callback functions when using an SSL-encrypted connection to the database server. These callbacks were not unregistered when the connection to the database was closed. If the calling application unloaded the libpq library after closing the connection, any subsequent attempt to use OpenSSL failed with a segmentation fault. To fix this problem, OpenSSL callbacks are now unregistered whenever the last active database connection is closed so that the library can be unloaded safely. OpenSSL Segmentation faults no longer occur in the scenario described.

All users of postgresql are advised to upgrade to these updated packages, which fix this bug.

4.148. postgresql84

4.148.1. RHSA-2011:1378 — Moderate: postgresql84 security update

Updated postgresql84 packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

PostgreSQL is an advanced object-relational database management system (DBMS).

Security Fix

CVE-2011-2483

A signedness issue was found in the way the crypt() function in the PostgreSQL pgcrypto module handled 8-bit characters in passwords when using Blowfish hashing. Up to three characters immediately preceding a non-ASCII character (one with the high bit set) had no effect on the hash result, thus shortening the effective password length. This made brute-force guessing more efficient as several different passwords were hashed to the same value.

Note

Due to the CVE-2011-2483 fix, after installing this update some users may not be able to log in to applications that store user passwords, hashed with Blowfish using the PostgreSQL crypt() function, in a back-end PostgreSQL database. Unsafe processing can be re-enabled for specific passwords (allowing affected users to log in) by changing their hash prefix to "$2x$".

These updated postgresql84 packages upgrade PostgreSQL to version 8.4.9. Refer to the PostgreSQL Release Notes for a full list of changes:

http://www.postgresql.org/docs/8.4/static/release.html

All PostgreSQL users are advised to upgrade to these updated packages, which correct this issue. If the postgresql service is running, it will be automatically restarted after installing this update.

4.149. ppc64-utils

4.149.1. RHEA-2012:0186 — ppc64-utils bug fix and enhancement update

An updated ppc64-utils package that fixes three bugs and adds two enhancements is now available for Red Hat Enterprise Linux 5.

The ppc64-utils package is a collection of utilities for Linux running on 64-bit PowerPC platforms.

Bug Fixes

BZ#666054

The help output of the "ls-vdev" command suggested using the "--version" and "--help" options although "ls-vdev" does not support these options. This update corrects the command help output so it displays only supported options, currently "-V" and "-h".

BZ#705012

The vscsisadmin utility and other tools installed by the ppc64-utils package relied on the obsolete ibmvscsis driver. Without the driver configured, the system displayed the following error on boot:

Starting ibmvscsisd: /etc/ibmvscsis.conf file does not exist. [FAILED]

This could have confused users. This update therefore removes these obsolete utilities from the ppc64-utils package, and the system no longer tries to initialize the ibmvscsisd service.

BZ#739706

The lsmcode tool provided incomplete information when it was used with with "-A, --All" or "-dDEV, --device=DEV" options. The lsmcode command help output and the lsmcode(8) manual page also described obsolete options, "-c, --no-menus" and "-r, --tabular". With this update, all aforementioned problems has been corrected, the command help output and manual page now provides only relevant information and lsmcode works as expected.

Enhancements

BZ#714179

The powerpc-utils component, which is a part of the ppc64-utils package, has been upgraded to upstream version 1.2.10. This update, among other changes, adjusts the ofpathname script to support and enable the SAS VRAID capability for IBM Power7 6Gb SAS PCIe Gen2 adapters.

BZ#651877

The upgraded powerpc-utils component introduces a new tool, lparstat, that allows to display various attributes and performance metrics of IBM Power Logical Partitions, which the tool collects from various system files, such as /proc/ppc64/lparcfg.

All users of ppc64-utils are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.150. procinfo

4.150.1. RHBA-2012:0021 — procinfo bug fix update

An updated procinfo package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The procinfo package contains a set of system utilities providing users with system information. The procinfo package includes the following commands: procinfo, lsdev, socklist.

Bug Fix

BZ#769857

Previously, the procinfo command calculated the system idle time in a way that caused arithmetic overflows. As a consequence, procinfo displayed the system idle time incorrectly, which eventually resulted in buffer overflows. With this update, procinfo has been modified to convert variables to a larger data type before they are used in the calculation so that procinfo now always displays the system idle time correctly. Buffer overflows no longer occur under these circumstances.

All users of procinfo are advised to upgrade to this updated package, which fixes this bug.

4.151. procps

4.151.1. RHEA-2011:1497 — procps enhancement update

An enhanced procps package is now available for Red Hat Enterprise Linux 5.

The procps package contains a set of system utilities that provide system information. The procps package includes the following commands: ps, free, skill, pkill, pgrep, snice, tload, top, uptime, vmstat, w, watch, and pdwx.

Enhancement

BZ#547749

Prior to this update the option to sort processes based on memory consumption using the top utility was only available in interactive mode (using Shift-M). Consequently you could not sort based on memory usage in batch mode. With this update an option, "-m", has been added to the "top" command that will automatically sort by memory usage.

Users of procps are advised to upgrade to this updated package, which adds this enhancement.

4.152. python

4.152.1. RHBA-2011:1319 — python bug fix update

Updated python packages that fix one bug are now available for Red Hat Enterprise Linux 5.

Python is an interpreted, interactive, object-oriented programming language. Python includes modules, classes, exceptions, high-level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems (X11, Motif, Tk, Mac and MFC).

Bug Fix

BZ#734005

The urllib.unquote method uses a dictionary containing pairs of hexadecimal values. Prior to this update, this dictionary only contained those combinations where the hexadecimal digits

were both upper case or lower case, omitting those pairs where one digit was upper case, the other lower case. As a result, percent-escape sequences containing both upper and lower case hexadecimal characters were not decoded in Python. This update modifies the dictionary creation code so that it includes keys for all combinations of upper and lower case hexadecimal digits. Now, all mixed-case hexadecimal digit pairs are correctly decoded by the urllib.unquote method.

All Python users are advised to upgrade to these updated packages, which fix this bug.

4.152.2. RHBA-2012:0297 — python bug fix update

Updated python packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

Python is an interpreted, interactive, object-oriented programming language. Python includes modules, classes, exceptions, high-level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems (X11, Motif, Tk, Mac and MFC).

Bug Fixes

BZ#732954

The urllib.unquote method uses a dictionary containing pairs of hexadecimal values. Prior to this update, this dictionary only contained those combinations where the hexadecimal digits were both upper case or lower case, omitting those pairs where one digit was upper case, the other lower case. As a result, percent-escape sequences containing both upper and lower case hexadecimal characters were not decoded in Python. This update modifies the dictionary creation code so that it includes keys for all combinations of upper and lower case hexadecimal digits. Now, all mixed-case hexadecimal digit pairs are correctly decoded by the urllib.unquote method.

BZ#708292

Prior to this update, python did not include an alias for "en_in" to convert "en_IN" into "en_IN.ISO8859-1". Consequently, the yum grouplist command would not work when the console LANG variable was set as follows: LANG=en_IN. With this update, an alias has been added in the locale.py file and yum grouplist now functions as expected with LANG=en_IN.

All Python users are advised to upgrade to these updated packages, which fix these bugs.

4.153. python-rhsm

4.153.1. RHBA-2012:0280 — python-rhsm bug fix update

An updated python-rhsm package that fixes several bugs is now available for Red Hat Enterprise Linux 5.

The python-rhsm package is a library for communicating with the REST interface of the Red Hat Unified Entitlement Platform. It provides access to the Subscription Management tools which help users to understand specific products which are installed on their machines and specific subscriptions which their machines consume.

Bug Fixes

BZ#720360

Previously, python-rhsm wrote entitlement certificate files that were readable by all users. Consequently, all users could view the system's entitlements by looking at the files. Now, python-rhsm writes certificates that are only readable by the root user. As a result, only root is able to view system entitlements using manual certificate inspection.

BZ#749853

The virt-who agent required new API calls to candlepin, the entitlement management system, for reporting the status of hypervisors and virtual guests. Without support in python-rhsm for these calls, virt-who would be unable to send the required information to candlepin. With this update, wrappers for these hypervisor-specific API calls have been added to python-rhsm. As a result, virt-who is able to pass hypervisor-specific information for host and guest entitlement management.

BZ#768983

Previously, if a system was subscribed to future-dated entitlements, the "subscription-manager repos --list" command showed the future-dated entitlement's repo in the repo list. This is incorrect and could be confusing to users. This has been corrected by performing a check for future-dated entitlements while iterating over the list of available repos. Users should no longer see future-dated entitlements when using the "repos --list" command directive.

All users of python-rhsm are advised to upgrade to this updated package, which fixes these bugs.

4.154. python-virtinst

4.154.1. RHBA-2012:0233 — python-virtinst bug fix update

An updated python-virtinst package that fixes three bugs is now available for Red Hat Enterprise Linux 5.

The python-virtinst package provides a Python module that helps build and install libvirt-based virtual machines.

Bug Fixes

BZ#704396

Running the "virt-install" command with the "--noapic" or "--noacpi" option overrides the operating system type so that it disables the Advanced Programmable Interrupt Controller (APIC) or Advanced Configuration and Power Interface (ACPI) setting on a fully virtualized guest. Previously, executing the command with the option mentioned did not take effect when installing a guest. A patch has been applied to address this issue, and running the "virt-install" command with the "--noapic" or "--noacpi" option specified works as expected.

BZ#704417

When cloning a KVM guest by using the virt-clone utility, the new MAC address was generated with an incorrect prefix. This was becasue the prefix allocated to Xen was used instead of the prefix allocated to QEMU. An upstream patch has been applied to address this issue, and the correct MAC prefix is now generated when cloning KVM guests.

BZ#706398

Previously, the maxnode variables returned for virtio, scsi or paravirtualized disks were hard-

coded to number 16. As a consequence, the virt-manager utility failed to add more than 16 paravirtualized disks, and displayed the following message:

no more space for disks of type xvd

This update increases the number to 1024. Users can now add more than 16 new storage devices successfully, without errors.

All users of python-virtinst are advised to upgrade to this updated package, which fixes these bugs.

4.155. PyXML

4.155.1. RHBA-2011:1460 — PyXML bug fix update

An updated PyXML package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

PyXML provides XML libraries for Python. The distribution contains a validating XML parser, an implementation of the SAX and DOM programming interfaces, and an interface to the Expat parser.

Bug Fixes

BZ#521307

Prior to this update, PyXML contained the shebang line, "#!/usr/bin/env python". This made it difficult to install alternative versions of Python on the system. With this update, the shebang lines in Python executables have been changed to, "#!/usr/bin/python", to ensure the Python interpreter installed on the system is used.

BZ#472009

Python packages provide extra metadata about the package in the form of eggs. Prior to this update, PyXML-0.8.4-py2.4.egg-info was missing. As a result, one of the scripts of the Zolera Soap Infrastructure (ZSI) Python module did not work correctly as it could not find the PyXML libraries. As a result of this update, the missing information has now been provided, the Python eggs are now built correctly, and python-ZSI module no longer fails at runtime.

All users of PyXML are advised to upgrade to this updated package, which fixes these bugs.

4.156. qt4

4.156.1. RHSA-2011:1324 — Moderate: qt4 security update

Updated qt4 packages that fix two security issues are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Qt 4 is a software toolkit that simplifies the task of writing and maintaining GUI (Graphical User Interface) applications for the X Window System. HarfBuzz is an OpenType text shaping engine.

Security Fixes

CVE-2007-0242

A flaw in the way Qt 4 expanded certain UTF-8 characters could be used to prevent a Qt 4 based application from properly sanitizing user input. Depending on the application, this could allow an attacker to perform directory traversal, or for web applications, a cross-site scripting (XSS) attack.

CVE-2011-3193

A buffer overflow flaw was found in the harfbuzz module in Qt 4. If a user loaded a specially-crafted font file with an application linked against Qt 4, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

Users of Qt 4 should upgrade to these updated packages, which contain backported patches to correct these issues. All running applications linked against Qt 4 libraries must be restarted for this update to take effect.

4.157. rdesktop

4.157.1. RHBA-2012:0213 — rdesktop bug fix update

An updated rdesktop package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The rdesktop package is an open source client for Windows NT Terminal Server and Windows 2000 & 2003 Terminal Services, capable of natively speaking Remote Desktop Protocol (RDP) in order to present the user's NT desktop.

Bug Fixes

BZ#581010

When using rdesktop to connect to a Windows Server 2008 R2 machine, the server generated a cursor-related command that rdesktop did not support. As a consequence, the mouse pointer was all black. This update applies an upstream patch to fix this issue and the mouse pointer is now white in color with a black border when connecting to a Windows Server 2008 R2 machine.

BZ#572287

When connecting to a Windows Server 2008 R2 machine, receiving a redirect could cause the rdesktop client to terminate unexpectedly with a segmentation fault. This update applies a patch that fixes this error, and receiving a redirect from a Windows Server 2008 R2 machine no longer causes rdesktop to crash.

All users of rdesktop are advised to upgrade to this updated package, which fixes these bugs.

4.158. redhat-release

4.158.1. RHEA-2012:0315 — redhat-release enhancement update

A new redhat-release package is now available for Red Hat Enterprise Linux 5.8.

The redhat-release package contains licensing information regarding, and identifies the installed version of, Red Hat Enterprise Linux.

This new package reflects changes made for the release of Red Hat Enterprise Linux 5.8.

Users of Red Hat Enterprise Linux 5.8 are advised to install this new package.

4.159. redhat-release-notes

4.159.1. RHEA-2012:0298 — redhat-release-notes enhancement update

An updated redhat-release-notes package is now available for Red Hat Enterprise Linux 5.8 as part of ongoing support and maintenance of Red Hat Enterprise Linux 5.

Red Hat Enterprise Linux minor releases are an aggregation of individual enhancement, security and bug fix errata. The Red Hat Enterprise Linux 5.8 Release Notes documents the major changes made to the Red Hat Enterprise Linux 5 operating system and its accompanying applications for this minor release. Detailed notes on all changes in this minor release are available in the Technical Notes.

This package contains the Release Notes for Red Hat Enterprise Linux 5.8.

The online Red Hat Enterprise Linux 5.8 Release Notes, which are located online at:

https://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/html/5.8_Rele ase_Notes/index.html

are to be considered the definitive, up-to-date version. Customers with questions about the release are advised to consult the online Release and Technical Notes for their version of Red Hat Enterprise Linux.

Users of Red Hat Enterprise Linux 5 are advised to upgrade to this updated redhat-release-notes package, which adds the updated Release Notes.

4.160. rgmanager

4.160.1. RHBA-2012:0066 — rgmanager bug fix update

An updated rgmanager package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The rgmanager package contains the Red Hat Resource Group Manager, which provides the ability to create and manage high-availability server applications in the event of system downtime.

Bug Fix

BZ#759542

Previously, rgmanager inappropriately called the rg_wait_threads() function during cluster reconfiguration. This could lead to an internal deadlock in rgmanager which caused the cluster services to become unresponsive. This irrelevant call has been removed from the code and deadlocks now no longer occur during cluster reconfiguration.

All users of rgmanager are advised to upgrade to this updated package, which fixes this bug.

4.160.2. RHBA-2012:0163 — rgmanager bug fix and enhancement update

An updated *rgmanager* package that fixes multiple bugs and adds one enhancement is now available for Red Hat Enterprise Linux 5.

The *rgmanager* package contains the Red Hat **Resource Group Manager**, which provides the ability

to create and manage high-availability server applications in the event of system downtime.

Bug Fixes

BZ#690265

When running a *Sybase database* on a cluster, the cluster defines the ASEHA (Sybase Adaptive Server Enterprise with the High Availability Option) resource agents to manage the Sybase cluster resources. The **ASEHAagent** resource agent previously specified all resource attributes as **unique**. As a consequence, it was difficult to have more than one **ASEHAagent** resource present in the cluster because the **Resource Group Manager** ignores all resources with conflicting "unique" attributes. This update removes the **unique** flag from all unnecessary attributes so it is now possible to run multiple **ASEHAagent** resource agents on one cluster node.

BZ#700103

Previously, **rgmanager** did not handle *wildcard characters* matching in the **nfsclient.sh** script correctly. Therefore, **rgmanager** was unable to detect removal of an NFS export from the export table if there was another NFS export which matched the wildcard pattern. Consequently, **rgmanger** did not restart the appropriate NFS service as expected. This update corrects wildcard matching logic so that **rgmanager** now correctly recognizes removal of matched NFS exports and restarts the relevant NFS service.

BZ#713243

Previously, **rgmanager** inappropriately called the **rg_wait_threads()** function during cluster reconfiguration. This could lead to an internal deadlock in **rgmanager**, which caused the cluster services to become unresponsive. This incorrect call has been removed from the code and deadlocks now no longer occur during *cluster reconfiguration*.

BZ#722230

Resource Group Manager did not properly handle *service status reporting* in certain situations within a *multi-node cluster* with a restricted failover domain defined. Consequently, if a service failover failed because there was an exclusive service running on the only suitable standby node, **rgmanager** reported the failed service as **started** on an offline node. This update modifies Resource Group Manager's event handling so a failed service is now correctly reported as **stopped** in this scenario.

BZ#743442

Resource Group Manager did not handle *inter-service dependencies* correctly. Therefore, if a service was dependent on another service that was running on the same cluster node, the dependent service became unresponsive during the service failover and remained in the **recovering** state. With this update, **rgmanager** has been modified to check a service state during failover and stop the service if it is dependent on the service that is failing over. **Resource Group Manager** then tries to start this dependent service on other nodes as expected.

BZ#752486

A rare race condition could occur when **rgmanager** received a request to start a new resource group thread while another thread was exiting. This race condition could cause a **Time of Check to Time of Use** (**TOC/TOU**) bug, which under certain circumstances resulted in an attempt to access previously-freed memory. As a consequence, **rgmanager** terminated

unexpectedly with a *segmentation fault*. To avoid the **TOC/TOU** problem, **rgmanager** now checks the status of the resource group thread before attempting to use the thread. This ensures that the thread is referred to correctly and **Resource Group Manager** thus no longer crashes in this scenario.

BZ#768146

Resource Group Manager fails to stop a resource if it is located on unmounted file system. As a result of this failure, **rgmanager** treated the resource as **missing** and marked the appropriate service as **failed**, which prevented the cluster from recovering the service. This update allows **rgmanager** to ignore this error if a resource has not been previously started with a service. The service can now be properly started on a different host.

BZ#743214

Under certain circumstances, a **stopped** event could be processed after a service and its dependent services had already been restarted. This forced the dependent services to be restarted erroneously. This update allows **rgmanager** to ignore the **stopped** events if dependent services have already been started and the services are no longer restarted unnecessarily.

BZ#769731

Due to changes in the behavior of the **LVM** commands, failed devices could not be removed from a **volume group** (**VG**) in the same way as previously. This resulted in an inability to relocate cluster services because the affected VG and **logical volumes** (**LV**s) could not be modified while the failed device was present in the VG. This update adds an additional command that is now needed in order to remove the failed physical volume from the VG. Services running on affected LVs can now be relocated correctly.

BZ#744283

When running multiple **oracledb** resource instances at the same time, several instances could attempt to write into a *shared log file* at the same moment. This caused all but one resource to fail and the log file to become *corrupted*. With this update, rgmanager now uses a unique log file per each **oracledb** resource instance.

Enhancement

BZ#747352

The **SAPDatabase** resource agent shipped with the Red Hat Enterprise Linux High Availability add-on was out of sync with the upstream version. This could cause **Resource Group Manager** to fail to manage **SAP** instances properly. This update applies multiple upstream patches, which provide several bug fixes and enhancements, including the following:

- The scope of the internal **rc** variable has been corrected in several internal functions.
- The Oracle recovery method has been changed from **recover automatic database** to **end backup**.
- The *process search pattern* has been adjusted for **DB2** version 9.5.
- The Oracle **listener** service is now started only if some database processes have been found.

- The **eval** command is no longer used to start a new process when unnecessary.

This updated **SAPDatabase** resource agent allows improved handling of *SAP database* instances in Red Hat cluster environment.

All users of *rgmanager* are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.161. rhn-client-tools

4.161.1. RHBA-2012:0250 — rhn-client-tools bug fix update

Updated rhn-client-tools packages that fix various bugs are now available for Red Hat Enterprise Linux 5.

The rhn-client-tools packages provide programs and libraries that allow a system to receive software updates from Red Hat Network (RHN) and Red Hat Network Satellite.

Bug Fixes

BZ#595837, BZ#751760

Prior to this update, the libraries provided by the rhn-client-tools packages may have occasionally failed with a traceback when the network connection was reset by peer. With this update, the underlying source code has been modified to display an appropriate error message in this situation.

BZ#706148

When more then one server was enabled in the /etc/sysconfig/rhn/up2date configuration file and the first server was not available, a yum command such as "yum update" did not attempt to connect to the second server and kept connecting to the first one. This update applies a patch that corrects this error, and when the first server is unavailable, yum now attempts to connect to the second server as expected.

BZ#720966

The rhn-channel utility allows users to subscribe or unsubscribe from a channel on the command line. Previously, an attempt to provide both username and password interactively caused the authentication to fail with the "Invalid username/password combination" error message. This happened, because rhn-channel did not remove the newline character from the username. With this update, this error has been corrected, and the rhn-channel utility no longer fails to authenticate the user when correct credentials are entered interactively.

BZ#729467

When a user runs the rhn_register utility on a system that is already registered, the utility displays a warning message that the system is already set up for software updates. This update rephrases this warning message for clarity.

BZ#744111

When a user registered a system with RHN Classic immediately after its provisioning, the Subscription Manager incorrectly reported that the system is non-compliant. Consequent to this,

the user had to log out and then log in to the system to work around this problem. With this update, when a user registers a system with RHN Classic, the Red Hat Network Client Tools now send a message to the Subscription Manager over D-Bus, resolving this issue.

BZ#773463

When using the firstboot application to register a system, "RHN Classic Mode" is now selected by default on the "Choose Server" screen.

BZ#681132

The underlying implementation of exception handling has been corrected.

All users of rhn-client-tools are advised to upgrade to these updated packages, which fix these bugs.

4.162. rhnlib

4.162.1. RHBA-2012:0240 — rhnlib bug fix update

An updated rhnlib package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The rhnlib package consists of a collection of Python modules used by the Red Hat Network (RHN) software.

Bug Fix

BZ#665026

Prior to this update, programs that used rhnlib were unable to connect to RHN or RHN Satellite using an IPv6 address. With this update, the underlying source code has been modified to correct this error, and rhnlib-based applications are now able to connect to RHN or RHN Satellite without any problems with IPv6 address resolution.

All users of rhnlib are advised to upgrade to this updated package, which fixes this bug.

4.163. rhpl

4.163.1. RHBA-2012:0275 — rhpl bug fix update

An updated rhpl package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The rhpl package contains a library of Python code used in programs throughout Red Hat Enterprise Linux.

Bug Fix

BZ#669666

When a user attempted to rebuild the rhpl package with version 0.17 of the gettext package that is shipped with Red Hat Enterprise Linux 5, the make command failed with the following error:

xgettext: Non-ASCII string at ../src/gzread.py:60.

With this update, this error no longer occurs and the rhpl package can now be rebuilt as

expected.

All users of rhpl are advised to upgrade to this updated package, which fixes this bug.

4.164. rng-utils

4.164.1. RHEA-2012:0293 — rng-utils enhancement update

An updated rng-utils package that adds one enhancement is now available for Red Hat Enterprise Linux 5.

The rng-utils package provides random number generator utilities for user space, such as the rngd daemon.

Enhancement

BZ#754290

A new "-i" (or "--ignorefail") command line option is now supported by the rngd daemon. This option allows rngd to ignore repeated warning messages about failed FIPS checks. Additionally, the rngd(8) manual page has been updated to provide a description of this newly added option.

All users of rng-utils are advised to upgrade to this updated package, which adds this enhancement.

4.165. rpm

4.165.1. RHSA-2011:1349 — Important: rpm security update

Updated rpm packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4, 5, and 6, and Red Hat Enterprise Linux 3 Extended Life Cycle Support, 5.3 Long Life, 5.6 Extended Update Support, and 6.0 Extended Update Support.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The RPM Package Manager (RPM) is a command line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.

Security Fixes

CVE-2011-3378

Multiple flaws were found in the way the RPM library parsed package headers. An attacker could create a specially-crafted RPM package that, when queried or installed, would cause rpm to crash or, potentially, execute arbitrary code.

Note

Although an RPM package can, by design, execute arbitrary code when installed, this issue would allow a specially-crafted RPM package to execute arbitrary code before its digital signature has been verified. Package downloads from the Red Hat Network remain secure due to certificate checks performed on the secure connection.

All RPM users should upgrade to these updated packages, which contain a backported patch to correct these issues. All running applications linked against the RPM library must be restarted for this update to take effect.

4.165.2. RHBA-2012:0283 — rpm bug fix and enhancement update

Updated rpm packages that fix multiple bugs and add two enhancements are now available for Red Hat Enterprise Linux 5.

The RPM Package Manager (RPM) is a command-line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.

Bug Fixes

BZ#510469

Previously, an attempt to initialize the rpm database in a non-existent directory could have failed to create a transaction lock. With this update, this problem has been fixed in that RPM now tries to create a non-existent directory before creating the lock.

BZ#573043

Previously, an attempt to close a NULL rpmio file descriptor caused the process to terminate with when calling the "assert()" function. With this update, the problem with the process termination has been fixed and the "Fclose()" function now accepts a NULL pointer and performs no operation.

BZ#628883

Previously, in Python bindings, calling "hdr.dsFromHeader()" caused a SystemError exception on headers with no dependencies, for example gpg-pubkey headers. With this update, RPM now returns an empty dependency set object in this case.

BZ#673821

Previously, RPM library initialization forced the umask of the process to "022", which could have caused unwanted permissions for files created by software that makes use of the RPM API. With this update, the umask is now only changed for the duration of a transaction and restored to its previous value afterwards.

BZ#740345

Previously, disabling package scriptlet execution (the "rpm --noscripts" command) did not prevent "%pretrans" and "%posttrans" scriptlets from running. With this update, the "--noscripts" option now disables execution of all scriptlet types.

Enhancements

BZ#620674

The "%setup" and "%patch" spec directives now support transparent decompression of XZ and LZMA compressed source tarballs and patch files.

BZ#533831

Support for the "RPMCALLBACK_SCRIPT_ERROR" callback event has been added in this update. This allows programs that make use of the librpm API (for example yum) to report install or erase failures more accurately.

All users of RPM are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.166. rsh

4.166.1. RHBA-2011:1429 — rsh bug fix update

Updated rsh packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The rsh packages contain programs which allow users to run commands on remote machines, log in to other machines, copy files between machines (rsh, rlogin and rcp), and provide an alternate method of executing remote commands (rexec). All of these programs are run by the xinetd daemon and can be configured using the Pluggable Authentication Modules (PAM) system and configuration files in the /etc/xinetd.d/ directory.

Bug Fix

BZ#749322

The rshd daemon performed redundant calls of the setpwent and endpwent functions. As a consequence, rshd queried NIS servers with every rsh access. With this update, these redundant calls were removed so that rshd no longer contacts NIS servers unnecessarily.

All users of rsh are advised to upgrade to these updated packages, which fix this bug.

4.167. rsync

4.167.1. RHBA-2011:1112 — rsync bug fix update

An updated rsync package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The rsync tool is used to copy and synchronize files locally or across a network. The rsync works very fast because it uses delta encoding and sends just differences in files instead of whole files. The rsync is also used as powerful mirroring tool.

Bug Fix

BZ#726060

The RHSA-2011-0999 - Moderate: rsync security, bug fix and enhancement update, which was applied with the rsync tool update to version 3.0.6-4, introduced a patch which fixed the issue

with missing memory deallocation. Due to an error in that patch, the following new issue appeared: when specifying the source or destination argument of the rsync command without the optional user@ argument, rsync failed to provide the correct parameters to an external command, such as ssh, and thus rsync failed with an error. With this update, the source code has been modified to fix this issue.

All users of rsync are advised to upgrade to this updated package, which resolves this issue.

4.168. rsyslog

4.168.1. RHBA-2012:0228 — rsyslog bug fix and enhancement update

Updated rsyslog packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

The rsyslog packages provide an enhanced, multi-threaded syslog daemon. It supports MySQL, syslog/TCP, RFC 3195, permitted sender lists, filtering on any message part, and fine grain output format control.

Bug Fixes

BZ#592039, BZ#582288

Previously, rklogd, the daemon that provides kernel logging, was replaced with a loadable module. However, the functionality was disabled in the configuration. Consequently, rsyslog did not log any kernel messages. With this update, the /etc/rsyslog.conf configuration file has been corrected to include the "$ModLoad imklog" directive and the kernel messages are now logged as expected.

BZ#674450

The previous version of rsyslog introduced a patch, which fixed unexpected termination that occurred when a large number of clients was sending their logs to rsyslog. However, the patch was not applied due to the outdated Autoconf package in the build environment. With this update, the package is no longer needed during the build process and the patch is applied successfully.

BZ#583621

The previous rsyslog release introduced a new format of the message time stamps. However, some utilities, such as logwatch, were unable to parse such message time stamps properly. This update adds the "$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat" directive to the /etc/rsyslog.conf configuration file so that the old format is used by default and the respective utilities now work correctly.

BZ#546645

Previously, some rsyslog modules were stored in the /usr/lib{,64} directory tree. Consequently, rsyslog could fail to start if the /usr/ directory resided on a different file system and the file system was unavailable during the daemon startup. With this update, the module directory has been relocated to the /lib{,64}/ directory and the modules are always accessible to rsyslog.

BZ#601711

The omsnmp module was missing in the rsyslog package. Consequently, sending of messages with Simple Network Management Protocol (SNMP) could not be used. This update adds the omsnmp module to the package and the SNMP messages mechanism works as expected.

BZ#746179

Wrong data types were used to hold some configuration values, which caused rsyslog to ignore the values. This update changes the data types and the configuration is now processed as expected.

BZ#726525

The retry limit was not checked correctly and suspended actions could fail to resume. This update fixes the underlying code and suspended actions resume as expected.

BZ#654379

The rsyslog utility failed to close the stdout and stderr streams properly when running in background mode. This caused the operating system to become unresponsive on system boot. The output streams are now closed properly, which fixes this bug.

BZ#637959

The rsyslog process could consume excessive memory when using message forwarding with Transport Layer Security (TLS) encryption. With this update, the underlying code has been modified and the bug is fixed.

BZ#694413

The build script wrongly detected the MySQL support when building 32-bit packages in a 64-bit multilib environment. Consequently, the building process failed. With this update, the build script now uses the proper mysql_config binary and the package is built successfully in this scenario.

BZ#650509

The lock file created by the rsyslog init script did not match the init script name. Consequently, the system did not run the stop action to stop the process on system shut down. With this update, the file is named correctly and the daemon shuts down as expected.

Enhancement

BZ#574620

This update improves the package description in the 'Description' section.

All rsyslog users are advised to upgrade to these updated packages, which fix these bugs and adds this enhancement.

4.169. ruby

4.169.1. RHBA-2012:0218 — ruby bug fix update

Updated ruby packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to do system management tasks.

Bug Fixes

BZ#435631

To identify the current working directory, the Ruby virtual machine used the path_check_0() function that recursed until it identified the respective absolute path. Previously, the function could cause the Ruby virtual machine to recurse infinitely and consume excessive memory. This happened if the environment path was broken as the getcwd() function failed to determine the full path of the current working directory. This update backports the non-recursive implementation of the path_check_0() function from Ruby 1.8.6, which relies on a series of macros, and the path_check_0() function returns the correct current working directory under these circumstances.

BZ#510277

The ruby update released on 2009-07-02 as RHSA-2009:1140 included a fix for CVE-2009-1904. This fix introduced a regression which caused leading zeros after the decimal point in BigDecimal objects to be dropped. This could, potentially, lead to incorrect mathematical calculations. This update fixes this problem by ensuring that leading zeros following a decimal point in BigDecimal objects are not dropped.

BZ#445399

Due to the missing "require 'rdoc/usage'" statement in the RI (Ruby Index) library, which is part of the ruby package, the Ruby virtual machine could raise the following exception:

uninitialized constant RI::Paths (NameError)

This update adds the missing require statement to the ri_options.rb file of the RI library file and the problem no longer occurs.

BZ#577351

The "Text::normalize" method included in the REXML (Regular Expressions XML) library, which is part of the Ruby standard library, did not work correctly for ampersand entities (&). With this update, the underlying "REXML::Text" class in the text.rb library has been modified and the ampersand characters are now normalized correctly.

All ruby users are advised to upgrade to these updated packages, which fix these bugs.

4.170. s390utils

4.170.1. RHBA-2012:0243 — s390utils bug fix update

An updated s390utils package that fixes multiple bugs is now available for Red Hat Enterprise Linux 5.

The s390utils package provides a set of utilities and daemons related to Linux for the IBM System z architecture.

Bug Fixes

BZ#705400

Prior to this update, the dasdinfo utility always returned a zero value even if an action failed. As a consequence, the return value could not be used if dasdinfo was used in a script. This update modifies the underlying code so that dasdinfo now returns a non-zero value if an error has occurred.

BZ#711774

Prior to this update, the lsluns utility always filtered for logical unit numbers (LUN) with the values 0xc101000000000000 or 0x0. As a consequence, the lsluns option "-a" listed only active LUNs with the values 0xc101000000000000 or 0x0. This update modifies the underlying code so that "-a" option no longer filters LUNs.

BZ#718696

Prior to this update, the cpuplugd utility failed to do a sanity check if the cpu/cmm_max value was greater than the cpu/cmm_min value. As a consequence, no action was performed. This update adds sanity checks for situations where the cpu/cmm_max value is greater than the cpu/cmm_min value.

BZ#718744

Prior to this update, the cpuplugd utility encountered a race condition when running the daemon and checking or creating the process ID (PID) file. As a consequence, multiple cpuplugd instances could be started concurrently. This update uses the flock() function when checking or creating the PID file and starting the daemon.

BZ#729609

Prior to this update, the fdasd check for a valid volume label did not correctly differentiate between interactive and non-interactive usage. As a consequence, the fdasd options "-config" and "-auto" on a device without a valid disk label could stop with the question "Should I create a new one? (y/n)" or completely fail with the message "Disc does not contain a VOL1 label, cannot create partitions". This update modifies the checking mechanism and fdasd now generates valid volume labels as expected.

BZ#730371

Prior to this update, the lsluns utility help contained the invalid "--ports" option. This update corrects the misprint so that lslun now uses the valid "--port" option.

BZ#736398

Prior to this update, the getharp utility terminated with the error "buffer overflow detected" if qetharp was invoked with an invalid interface name longer than 16 bytes. This update checks the length of a given interface name parameter. Now, getharp no longer encounters overflows in such situations.

BZ#738342

Prior to this update, the lsluns utility did not check whether the required SCSI generic (sg) functionality was available. As a consequence, lsluns failed silently if the sg functionality was unavailable. This update modifies the underlying code so that lsluns now checks for the availability and prints an error message if the sg functionality is not available.

All users of s390utils are advised to upgrade to this updated package, which fixes these bugs.

4.171. sabayon

4.171.1. RHBA-2012:0202 — sabayon bug fix update

Updated sabayon packages that fix three bugs are now available for Red Hat Enterprise Linux 5.

Sabayon is a tool to help system administrators and users change and maintain the default behaviour of the GNOME desktop. These packages contain the graphical tools which a system administrator uses to manage Sabayon profiles.

Bug Fixes

BZ#505402

Prior to this update, several GConf directories were listed in the list of folders to ignore. As a consequence, changes in the Mandatory GConf settings were not saved. This update removes these entries from the list. Now, all changes are saved as expected.

BZ#654569

Prior to this update, Sabayon terminated unexpectedly while attempting to save the profile if the user created a file or a directory on the desktop that contained an apostrophe in the name. With this update, any apostrophe characters in the name are now escaped so that Sabayon no longer terminates and correctly saves the profile.

BZ#660620

Prior to this update, the .config and .local directories were wrongly listed in the list of ignored directories. As a consequence, some settings could be lost. This update removes these entries from the list. Now, the configuration is saved correctly.

All sabayon users are advised to upgrade to these updated packages, which fix these bugs.

4.172. samba

4.172.1. RHSA-2011:1219 — Moderate: samba security update

Updated samba packages that fix multiple security issues are now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Samba is a suite of programs used by machines to share files, printers, and other information.

Security Fixes

CVE-2011-2694

A cross-site scripting (XSS) flaw was found in the password change page of the Samba Web Administration Tool (SWAT). If a remote attacker could trick a user, who was logged into the SWAT interface, into visiting a specially-crafted URL, it would lead to arbitrary web script

execution in the context of the user's SWAT session.

CVE-2011-2522

It was found that SWAT web pages did not protect against Cross-Site Request Forgery (CSRF) attacks. If a remote attacker could trick a user, who was logged into the SWAT interface, into visiting a specially-crafted URL, the attacker could perform Samba configuration changes with the privileges of the logged in user.

CVE-2010-0787

A race condition flaw was found in the way the mount.cifs tool mounted CIFS (Common Internet File System) shares. If mount.cifs had the setuid bit set, a local attacker could conduct a symbolic link attack to trick mount.cifs into mounting a share over an arbitrary directory they were otherwise not allowed to mount to, possibly allowing them to escalate their privileges.

CVE-2010-0547

It was found that the mount.cifs tool did not properly handle share or directory names containing a newline character. If mount.cifs had the setuid bit set, a local attacker could corrupt the mtab (mounted file systems table) file via a specially-crafted CIFS share mount request.

CVE-2011-1678

It was found that the mount.cifs tool did not handle certain errors correctly when updating the mtab file. If mount.cifs had the setuid bit set, a local attacker could corrupt the mtab file by setting a small file size limit before running mount.cifs.

Note

mount.cifs from the samba packages distributed by Red Hat does not have the setuid bit set. We recommend that administrators do not manually set the setuid bit for mount.cifs.

Red Hat would like to thank the Samba project for reporting CVE-2011-2694 and CVE-2011-2522; the Debian Security Team for reporting CVE-2010-0787; and Dan Rosenberg for reporting CVE-2011-1678. Upstream acknowledges Nobuhiro Tsuji of NTT DATA Security Corporation as the original reporter of CVE-2011-2694; Yoshihiro Ishikawa of LAC Co., Ltd. as the original reporter of CVE-2011-2522; and the Debian Security Team acknowledges Ronald Volgers as the original reporter of CVE-2010-0787.

Users of Samba are advised to upgrade to these updated packages, which contain backported patches to resolve these issues. After installing this update, the smb service will be restarted automatically.

4.172.2. RHSA-2012:0313 — Low: samba security, bug fix, and enhancement update

Updated samba packages that fix one security issue, one bug, and add one enhancement are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

Samba is an open-source implementation of the Server Message Block (SMB) or Common Internet File System (CIFS) protocol, which allows PC-compatible machines to share files, printers, and other information.

Security Fix

CVE-2010-0926

The default Samba server configuration enabled both the "wide links" and "unix extensions" options, allowing Samba clients with write access to a share to create symbolic links that point to any location on the file system. Clients connecting with CIFS UNIX extensions disabled could have such links resolved on the server, allowing them to access and possibly overwrite files outside of the share. With this update, "wide links" is set to "no" by default. In addition, the update ensures "wide links" is disabled for shares that have "unix extensions" enabled.

Warning

This update may cause files and directories that are only linked to Samba shares using symbolic links to become inaccessible to Samba clients. In deployments where support for CIFS UNIX extensions is not needed (such as when files are exported to Microsoft Windows clients), administrators may prefer to set the "unix extensions" option to "no" to allow the use of symbolic links to access files out of the shared directories. All existing symbolic links in a share should be reviewed before re-enabling "wide links".

Bug Fix

BZ#768908

The smbclient tool sometimes failed to return the proper exit status code. Consequently, using smbclient in a script caused some scripts to fail. With this update, an upstream patch has been applied and smbclient now returns the correct exit status.

Enhacement

BZ#736124

With this update, support for Windows Server 2008 R2 domains has been added.

Users are advised to upgrade to these updated samba packages, which correct these issues and add this enhancement. After installing this update, the smb service will be restarted automatically.

4.173. samba3x

4.173.1. RHSA-2011:1220 — Moderate: samba3x security update

Updated samba3x packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Samba is a suite of programs used by machines to share files, printers, and other information.

Security Fixes

CVE-2011-2694

A cross-site scripting (XSS) flaw was found in the password change page of the Samba Web Administration Tool (SWAT). If a remote attacker could trick a user, who was logged into the SWAT interface, into visiting a specially-crafted URL, it would lead to arbitrary web script execution in the context of the user's SWAT session.

CVE-2011-2522

It was found that SWAT web pages did not protect against Cross-Site Request Forgery (CSRF) attacks. If a remote attacker could trick a user, who was logged into the SWAT interface, into visiting a specially-crafted URL, the attacker could perform Samba configuration changes with the privileges of the logged in user.

CVE-2011-2724

It was found that the fix for CVE-2010-0547, provided by the Samba rebase in RHBA-2011:0054, was incomplete. The mount.cifs tool did not properly handle share or directory names containing a newline character, allowing a local attacker to corrupt the mtab (mounted file systems table) file via a specially-crafted CIFS (Common Internet File System) share mount request, if mount.cifs had the setuid bit set.

CVE-2011-1678

It was found that the mount.cifs tool did not handle certain errors correctly when updating the mtab file. If mount.cifs had the setuid bit set, a local attacker could corrupt the mtab file by setting a small file size limit before running mount.cifs.

Note

mount.cifs from the samba3x packages distributed by Red Hat does not have the setuid bit set. We recommend that administrators do not manually set the setuid bit for mount.cifs.

Red Hat would like to thank the Samba project for reporting CVE-2011-2694 and CVE-2011-2522, and Dan Rosenberg for reporting CVE-2011-1678. Upstream acknowledges Nobuhiro Tsuji of NTT DATA Security Corporation as the original reporter of CVE-2011-2694, and Yoshihiro Ishikawa of LAC Co., Ltd. as the original reporter of CVE-2011-2522.

Users of Samba are advised to upgrade to these updated packages, which contain backported patches to resolve these issues. After installing this update, the smb service will be restarted automatically.

4.173.2. RHBA-2012:0156 — samba3x bug fix and enhancement update

Updated *samba3x* packages that fix several bugs and provide multiple enhancements are now available for Red Hat Enterprise Linux 5.

Samba is an open-source implementation of the Server Message Block (SMB) or Common Internet File System (CIFS) protocol, which allows PC-compatible machines to share files, printers, and other

information.

Upgrade to an upstream version

The *samba3x* package has been upgraded to upstream version 3.5.10, which provides a number of bug fixes and enhancements over the previous version. In particular, this upgrade includes improvements to **ntlm_auth** for dealing with wrong passwords and repeated authentication attempts. As a result **ntlm_auth** now operates reliably, including with older Domain Controllers. (BZ#719369, BZ#593825, BZ#713466)

Bug Fixes

BZ#716182

If plain text passwords were used by setting ***encrypt passwords = no*** in **/etc/samba/smb.conf**, **Samba** clients running on the **Windows XP** or **Windows Server 2003** operating system may not have been able to access **Samba** shares after installing Microsoft Security Bulletin MS11-043. This update corrects this bug, allowing such clients to use plain-text passwords to access **Samba** shares.

BZ#719852

Samba failed to verify **Kerberos** authentication of an SMB Session Setup from a **Windows Vista** or **Windows Server 2008** *Common Internet File System*(CIFS) client when the **Kerberos** ticket size was greater than 16 KB. Consequently, if the connecting account was a member of more than 500 security groups, and the domain was configured to create tickets greater than 12Kb, authentication failed. The following error message was logged:

```
Failed to verify incoming ticket with error NT_STATUS_LOGON_FAILURE!
```

An upstream patch has been applied and **Samba** can now use **Kerberos** authentication for **Windows Vista** or **Windows Server 2008** CIFS clients in the scenario described.

BZ#725875

Previously, in certain environments with many users, the **pam_winbind** module stopped operating. As a result, failures occurred when users attempted to log in. With this update, the bug has been fixed so that **pam_winbind** now works as expected in the scenario described.

BZ#735165

The *group ID* (GID) of **ServerName\None** was incremented every time the *Identity Mapping* (IDMAP) cache expired. Given enough time the GID would eventually reach the top of the range specified by the ***idmap gid*** directive in the **smb.conf** file. Consequently, new allocation of GIDs would not be possible and a group would no longer resolve properly. This update includes an upstream fix and the cache expiry no longer causes GIDs to increment.

BZ#736375

The Name Service Switch daemon **winbind** produces excessive debug output messages when attempting to register an already-registered IDMAP module. Previously, the messages were set to debug level **0**. Consequently, the messages could not be filtered by lowering the ***log level*** parameter in **smb.conf**. With this update, a patch has been applied to increase the

debug level of the messages to **5**. As a result, the debug messages can now be filtered by setting the **smb.conf *log level*** parameter.

BZ#743467

If Linux clients used the CIFS client in the kernel to mount a **Samba** share, the ***force create mode*** parameter was not honored properly. As a result, files created on a mounted **Samba** share did not properly follow the ***umask*** parameter, and files with undesired permissions were created. With this update, the bug has been fixed and files are now created with the correct permissions.

BZ#743895

Due to a regression in **Samba**, **Windows Internet Explorer 9** running on **Windows 7** could not download files to a **Samba** share. Consequently, some Windows 7 users could not make use of **Samba** shares. This update includes upstream improvements to **Samba** to address this bug. As a result, **Windows 7** users can now save files on **Samba** shares using **Internet Explorer 9**.

BZ#747153

Previously, the man pages for certain **Samba** components did not document that primary group membership is not calculated based on the ***gidNumber*** LDAP attribute if Windows Services for UNIX (SFU) are enabled, or if the standard RFC 2307 LDAP attributes in the *Active Directory* (AD) are used. Instead, **Winbind** uses the ***primaryGroupID*** LDAP attribute. With this update, the man pages have been updated accordingly to reflect the aforementioned limitation.

BZ#748515

Previously, extracting files from a ZIP archive failed on the *Distributed File System* (DFS) shares if the following **symlinks = yes** parameter was not set. This bug has been fixed in this update so that extracting files from a ZIP archive now works as expected.

BZ#753828

If **winbind** was joined to the domain with ***idmap_ad*** specified as the backend, enumerating users was enabled, and most of the users had UIDs, then when calling **getent passwd** for a user who had no UID, the enumeration stopped and the following error was displayed:

```
NT_STATUS_NONE_MAPPED
```

This update implements an upstream patch to correct the problem. As a result, if a user cannot be mapped, **winbind** no longer stops but continues enumerating users in the scenario described.

BZ#754154

Previously, the **winbindd-locator** tool could not correctly find a *Domain Controller* (DC) using **Samba** and DNS SRV records when outside the networks that are known to AD and are mapped to AD sites. Consequently, when a host was a member of a **Windows Server 2008 R2** domain, and the host was in a network that was not mapped to any known site of the AD, the host could not locate a DC and an error message in the following format was logged:

```
ads_dns_lookup_srv: Failed to resolve
_ldap._tcp._sites.dc._msdcs.AD.EXAMPLE.COM
```

With this update a patch has been applied and **winbindd-locator** can now locate a DC in the scenario described.

BZ#755346

The **smbclient** tool sometimes failed to return the expected exit status code; it returned **0** instead of **1**. Consequently, using **smbclient** in a script caused some scripts to fail. With this update, an upstream patch has been applied and **smbclient** now returns the correct exit status.

BZ#766497

Previously, the **Winbind** IDMAP interface cache did not expire as specified in the **smb.conf** file. Consequently, the positive and negative entries in the cache would not expire until the opposite type of query was made. This update contains a backported fix for the problem. As a result, the ***idmap cache time*** and ***idmap negative cache time*** directives now work as expected.

BZ#771375

Previously, the net(8) man page did not document the **-k** option for using **Kerberos** authentication. Consequently, users were not aware how to use **Kerberos** authentication with the **net** utility. This update adds the missing documentation to the man page.

Users of *samba3x* should upgrade to these updated packages, which fix these bugs and add these enhancements.

4.174. sblim

4.174.1. RHBA-2012:0191 — sblim bug fix and enhancement update

Updated sblim packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

Standards-Based Linux Instrumentation for Manageability (SBLIM) consists of a set of standards-based, Web-Based Enterprise Management (WBEM) modules that use the Common Information Model (CIM) standard to gather and provide systems management information, events, and methods to local or networked consumers via an CIM object services broker using the CMPI (Common Manageability Programming Interface) standard. This package provides a set of core providers and development tools for systems management applications.

Bug Fixes

BZ#711423

The sblim-gather-provider package is DSP1053 compliant and advertises this via the Linux_MetricRegisteredProfile class under the root/interop namespace. Prior to this update, the registration of this class and provider was missing, preventing communication with the class via CIM object managers. With this update, the Linux_MetricRegisteredProfile class provider is properly registered under the root/interop namespace.

BZ#711193

Previously, CIM Metrics providers specific to IBM System z in the sblim-gather package were patched to workaround a bug in the 2.0.0 sysfs library. (The 2.0.0 sysfs library re-write inadvertently left out several API functions, including one -- open_device_tree -- the SBLIM Data Gatherer was dependent on.) Between the previous fence-agents release and this update, the sysfs library was updated to version 2.1.0 and that update restored the missing API interfaces, including open_device_tree. The patch which allowed sblim-gather-provider to work with sysfs library 2.0.0 does not work with 2.1.0, however. This update removes this patch, ensuring the CIM Metrics providers use the restored sysfs library APIs and providing full functionality, as expected.

Enhancements

BZ#713989

The sblim-cmpi-base packages have been updated to upstream version 1.6.1, which provides a number of bug fixes over the previous version.

BZ#713974

The sblim-gather packages have been updated to upstream version 2.2.3, which provides a number of enhancements over the previous version.

BZ#713985

The sblim-cmpi-fsvol packages have been updated to upstream version 1.5.1, which fixes a problem with incorrect fsvol registration.

BZ#713986

The sblim-cmpi-nfsv3 packages have been updated to upstream version 1.1.1. With this update, actual runtime settings of the nfsd tool are exposed, not only the static content of the /etc/exports file.

BZ#713973

The sblim-sfcb packages have been updated to upstream version 1.3.11, which provides a number of bug fixes and enhancements over the previous version.

BZ#716027

The sblim-sfcc packages have been updated to upstream version 2.2.2, which provides one bug fix over the previous version.

All sblim users should upgrade to these updated packages, which fix these bugs and add these enhancements.

4.175. scsi-target-utils

4.175.1. RHBA-2012:0279 — scsi-target-utils bug fix update

An updated scsi-target-utils package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The scsi-target-utils package contains the daemon and tools used to set up iSCSI and the iSCSI Extensions for RDMA (iSER) targets.

Bug Fix

BZ#742640

Prior to this update, scsi-target-utils could, under certain circumstances, terminate unexpectedly with a segmentation fault when the tgt daemon was stopped. This bug has been fixed in the code and scsi-target-utils no longer crashes in the described scenario.

All users of scsi-target-utils are advised to upgrade to this updated package, which fixes this bug.

4.176. selinux-policy

4.176.1. RHBA-2012:0106 — selinux-policy bug fix update

Updated selinux-policy packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

Bug Fix

BZ#784782

With SELinux in enforcing mode, an Open MPI (Message Passing Interface) job submitted to the parallel universe environment failed when an attempt to generate SSH keys with the ssh-keygen utility was made. With this update, the "ssh_keygen_t" SELinux domain type has been implemented as unconfined, which ensures the ssh-keygen utility to work correctly.

All users of selinux-policy are advised to upgrade to these updated packages, which fix this bug.

4.176.2. RHBA-2012:0158 — selinux-policy bug fix and enhancement update

Updated *selinux-policy* packages that fix a number of bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The *selinux-policy* packages contain the rules that govern how confined processes run on the system.

Bug Fixes

BZ#693149

When SELinux was running in the Enforcing mode, an incorrect SELinux policy prevented the **`wpa_cli`** client utility to connect to the running **`wpa_supplicant`** daemon. With this update, the SELinux policy has been fixed, and **`wpa_cli`** now works as expected.

BZ#715227

Due to an incorrect SELinux policy, the **`smartd`** daemon was not able to set up an monitor of a 3ware device. This update corrects this bug by adding an appropriate policy, which allows the **`smartd`** policy to create a fixed disk device node.

BZ#716956

Previously, the SELinux Multi-Level Security (MLS) policy did not allow the **cron** daemon to read a Kerberos configuration file. This update fixes the relevant SELinux policy to make sure the Kerberos configuration file can be read by the **cron** daemon.

BZ#717152

When the SELinux Multi-Level Security (MLS) policy was enabled, starting the **smartd** daemon caused Access Vector Cache (AVC) messages to be written to the **audit** log file. With this update, the relevant policy has been fixed and the AVC messages are no longer produced in the described scenario.

BZ#721041

When SELinux was running in the Enforcing mode, an incorrect SELinux policy prevented the **samba** service from scanning the **/boot/** directory when responding to quota check requests. The error has been fixed and **samba** is now allowed to search all mount points in the system.

BZ#722536

Previously, the **rsyslogd** daemon was unable to connect to a MySQL database when support for the *rsyslog-mysql* package was enabled. This bug has been fixed and **rsyslogd** is now allowed to connect to MySQL as expected.

BZ#722579

Due to an error in a SELinux policy, SELinux incorrectly prevented the **ricci** service from installing RPM packages. With this update, the fixed SELinux rules, which allow **ricci** to install RPM packages, have been provided.

BZ#728957

Previously, due to an incorrect SElinux context, the user was unable to access the **fetchmail.log** in their home directory. This update adds a SELinux security context for the **.fetchmailrc** file located in user home directories to allow the **fetchmail** application to get external private emails.

BZ#730294

Due to incorrect SELinux policy rules, the **procmail** mail delivery agent was not allowed to execute the **hostname** command when **HOST_NAME=`hostname`** was specified in the configuration file. This update adapts the SELinux policy to support this **procmail** option.

BZ#730962

When PAM (Pluggable Authentication Modules) authentication was used in the **squid** daemon with SELinux enabled, the AVC message related to the **netlink_audit_socket** SELinux class was written to the **audit** log file. With this update, the relevant policy has been fixed and using PAM with **squid** no longer produces these messages.

BZ#721041

When SELinux was running in the Enforcing mode, an incorrect SELinux policy prevented the **swat** (Samba Web Administration Tool) utility from writing to **samba** log files. This bug has been fixed and **swat** is now allowed to write to all **samba** log files.

BZ#733668

On a MLS system, if a new user attempted to reset their password on the first login, SELinux prevented this action. With this update, the SELinux policy has been updated to allow the **sysadm_t** SELinux user type transition to the **passwd_t** SELinux domain, which is intended for the **passwd** utility.

BZ#735813

Previously, the **/etc/passwd.adjunct** file contained an incorrect label, resulting in a wrong SELinux security context. This update adds a SELinux security context for **/etc/passwd.adjunct** to make it possible to use this file on a Network Information Service (NIS) server.

BZ#745139

When SELinux was running in the Enforcing mode, **rsyslog** clients were incorrectly denied access to port 6514 (**syslog-over-TLS**). This update adds a new SELinux policy that allows **rsyslog** clients to connect to this port.

BZ#745175

With the **omsnmp** module enabled, the latest version of the **rsyslog** daemon can send log messages as SNMP traps. This update adapts the SELinux policy to support this new functionality.

BZ#746351, BZ#761592

When SELinux was enabled, starting the **ricci** daemon caused Access Vector Cache (AVC) messages to be written to the **audit** log file. With this update, the relevant policy has been fixed and starting **ricci** no longer produces these messages.

BZ#752487

Due to inccorect SELinux policy, the **finger** application was not able to use the **nss_ldap** module to get information (such as users, hosts, and groups) from LDAP directories. With this update, fixed SELinux rules, which allow **finger** to connect to the LDAP port to get all needed information from LDAP, have been provided.

BZ#753039, BZ#767633

When an unconfined SELinux user runs the **ssh-keygen** utility, the user is able to generate SSH keys anywhere. However, transition from the **unconfined_t** to the **ssh_keygen_t** domain prevented this functionality. To make the **ssh-keygen** utility work correctly at all times, the **ssh_keygen_t** SELinux domain type has now been provided as an unconfined type.

BZ#754121

When SELinux was running in the Enforcing mode, the **sssd** service was not allowed to create, delete, or read symbolic links in the **/var/lib/sss/pipes/private/** directory. This update fixes the relevant SELinux policy rules to allow **sssd** to perform these operations.

BZ#761481

When SELinux was running in the Enforcing mode, the **sssd** service did not work properly; if a user authenticated to the **sshd** service using the Generic Security Services Application Program Interface (GSSAPI), subsequent authentication attempts failed. This update adds an appropriate security file context for the **/var/cache/krb5cache/** directory, which allows **sssd** to work correctly in the described scenario.

BZ#761485, BZ#767565

Previously, the SELinux security context for the **iscsiuio** binary was not defined in the policy. Consequently, the operation of the **iscsid** daemon could experience problems. This update adds a SELinux security context for the **/sbin/iscsiuio** file to make **iscsid** run in the proper SELinux domain, thus fixing this bug.

BZ#766591

When SELinux was running in the Enforcing mode, the **pam_oddjob_mkhomedir** utility could not be run, home directories could not be created, and actions for the **oddjob** service were denied. With this update, the appropriate SELinux rule has been provided and SELinux no longer prevents **pam_oddjob_mkhomedir** from working correctly in the described scenario.

BZ#781477

Due to an incorrect SELinux policy, an attempt to use the **nice** utility to modify scheduling priority of the **openvpn** service failed. This update provides fixed SELinux rules, adds the **sys_nice** capability, and users are now allowed to modify the scheduling priority as expected.

Enhancements

BZ#709370

With this update, the new SELinux policy for **mcelog** service has been added to make **mcelog** work properly on SELinux Multi-Level Security (MLS) systems.

BZ#718219

The support for the **dkim-milter**, DKIM (DomainKeys Identified Mail) mail filter, application has been backported to the *selinux-policy* package in order to allow the Postfix email server to use it.

BZ#720462

With this update, the new SELinux policy for the Zarafa Open Source Email & Collaboration Software has been provided for *selinux-policy*.

BZ#724941

With this update, the new SELinux policy for the **subscription-manager** utility has been provided for *selinux-policy*.

BZ#741670

A new SELinux Boolean value, **dhcpc_exec_iptables**, has been added to allow the **dhcpd** daemon to execute **iptables** commands.

All users of *selinux-policy* are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.177. sendmail

4.177.1. RHBA-2011:1127 — sendmail bug fix update

Updated sendmail packages that resolve an issue are now available for Red Hat Enterprise Linux 5.

Sendmail is a widely used Mail Transport Agent (MTA). MTAs deliver mail from one machine to another. Sendmail is not a client program, but rather a behind-the-scenes daemon that moves email over networks or the Internet to its final destination.

Bug Fix

BZ#726094

Sendmail previously used the MAXHOSTNAMELEN macro to allocate buffers containing host names and Fully Qualified Domain Names (FQDNs). The value of the MAXHOSTNAMELEN macro is set to 64 on Red Hat Enterprise Linux systems, which means that such allocated buffer can hold at most 63 characters, but according to the RFC1035, the FQDN maximal length is defined to 255 characters. This caused problems with a FQDN resolution in case that FQDN was longer then 63 characters. With this update, the code has been modified so that the size of buffers containing FQDN is now set to 256 bytes. The issues with the FQDN resolution now no longer occurs.

All users of sendmail are advised to upgrade to these updated packages, which resolve this issue.

4.178. setroubleshoot

4.178.1. RHBA-2012:0146 — setroubleshoot bug fix update

Updated setroubleshoot packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The setroubleshoot packages provide tools to help diagnose SELinux problems. When Access Vector Cache (AVC) messages are generated, an alert can be displayed that provides information about the problem and helps track its resolution. Alerts are user-configurable. The same tools can be run on existing log files.

Bug Fix

BZ#789143

Due to a memory leak in the rpm underlying code, the setroubleshoot tool consumed extensive memory resources. This update applies a patch that reduces memory consumption significantly, however, the problem has not been fixed completely and has to be resolved in the rpm utility.

All users of setroubleshoot are advised to upgrade to these updated packages, which fix this bug.

4.179. setup

4.179.1. RHBA-2012:0198 — setup bug fix and enhancement update

An updated setup package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The setup package contains a set of important system configuration and setup files, such as passwd, group, and profile.

Bug Fixes

BZ#501762

Prior to this update, the setup package did not reserve the group ID (GID) for the group wbpriv 88, used for sharing the permissions of sockets with Squid. As a consequence, other packages or system administrators could accidentally assign this group number to another group. With this update, the setup package reserves this GID name and number so that accidental conflicts with other users and groups no longer happen.

BZ#509919

Prior to this update, the /etc/hosts.deny configuration file contained an old comment about the redundant portmap line. This could cause confusion. With this update, this comment has been removed from the hosts.deny configuration file.

BZ#608987

Prior to this update, /etc/profile.d/ scripts umask modifications were not respected in the bash and the korn shell (ksh) login shell. This update corrects this behavior, so that umask modifications from /etc/profile.d scripts in bash and ksh login shell are again respected.

BZ#616116

Prior to this update, the /etc/profile script used the PS1 environmental variable for detecting interactive shell, which is not portable because this variable is set after the profile script execution the PS1 in the Korn shell. As a consequence, every ksh shell was treated as non-interactive and did not display the output from the profile.d scripts. This update uses a portable variable for interactive shell detection. Now, also ksh users can see the output of /etc/profile.d/ scripts in interactive shells.

BZ#617495

Prior to this update, /etc/profile.d/ scripts umask modifications were not respected in the tcsh login shell. With this update, all umask modifications from /etc/profile.d scripts in the tcsh login shell are again respected.

BZ#620443

Prior this update, /etc/bashrc script wrongly used two echo commands in PROMPT_COMMAND environment variable. As a consequence, the output of the terminal could, under certain circumstances, be placed into the terminal title. With this update, the bashrc script uses one single printf command in the PROMPT_COMMAND environment variable.

BZ#691430

Prior to this update, the PROMPT_COMMAND variable set by a custom profile.d script was overwritten with the default value from the /etc/bashrc script file. With this update, the /etc/bashrc script file has been updated so that it now respects a user-defined PROMPT_COMMAND variable, and does not overwrite it.

BZ#703051

Prior to this update, the /etc/host.conf file contained the redundant line "order host,bind", hwich the glibc library no longer uses. With this update, this line has been removed from the host.conf file.

BZ#760241

Prior to this update, the environmental variable PATH in the tcsh login shell contained remnants of the X11R6 hierarchy (/usr/X11R6/bin). This could confuse users because users of the bash/ksh login shell do not have this directory in PATH envvar. With this update, these remnants have been removed.

All users are advised to upgrade to this updated setup package, which fixes these bugs.

4.180. shadow-utils

4.180.1. RHBA-2012:0244 — shadow-utils bug fix update

An updated shadow-utils package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The shadow-utils package includes programs for converting UNIX password files to the shadow password format, as well as tools for managing user and group accounts.

Bug Fixes

BZ#619150

Prior to this update, the faillog utility executed command line options immediately after they were passed instead of parsing all options first. This update modifies the utility so that all command line options are parsed before executing the commands.

BZ#670364

Prior to this update, the faillog utility created huge /var/log/faillog files after setting the maximum number of login failures. This update fixes that behavior.

BZ#673091

Prior to this update, an attempt to copy the files of the /etc/skel/ directory with support for access control lists (ACLs) to a file system with disabled ACLs failed with the error: "copydir(): preserving permissions for /home/[username]/.kde: Operation not supported". This update modifies the ACLs so that the content of the /etc/skel/ directory is now successfully copied.

BZ#681020

Prior to this update, large user identifiers (UID) and group identifiers (GID) on 32-bit systems were not correctly handled. As a consequence, the pwconv and pwunconv utilities changed all identifiers greater than 2147483647 to this value. With this update, the underlying source code has been modified to ensure that the pwconv and pwunconv utilities no longer change the GIDs and UIDs.

BZ#688892

Prior to this update, the useradd(8) manual page contained incorrect information about the minimum numeric value for UIDs. This update lists now the correct minimum UID number of 500.

BZ#709605

Prior to this update, the useradd utility did not delete its lock files after an unsuccessful execution. This update modifies the utility so that lock files are now correctly deleted.

BZ#715214

Prior to this update, the groupadd manual page description of "-r" was only valid for the default value of GID_MIN. This update contains accurate information regardless of whether GID_MIN is left at the default value of 500.

All users of shadow-utils are advised to upgrade to this updated package, which fixes these bugs.

4.181. smartmontools

4.181.1. RHBA-2011:1784 — smartmontools bug fix update

An updated smartmontools package that fixes a bug is now available for Red Hat Enterprise Linux 5.

The smartmontools package contains two utilities, smartctl and smartd, that enable the controlling and monitoring of Self-Monitoring, Analysis and Reporting Technology System (S.M.A.R.T.) enabled storage systems. These utilities provide advanced warning of disk degradation and failure.

Bug Fix

BZ#714888

Prior to this update, the format in which certain HP SAS (Serial Attached SCSI) drives returned S.M.A.R.T. data was not recognized by smartmontools and the following error message "scsi response fails sanity test" was logged. With this update, smartmontools now correctly recognizes the data and this error no longer occurs.

All users of smartmontools are advised to upgrade to this updated package, which fixes this bug.

4.182. sos

4.182.1. RHBA-2011:1535 — sos bug fix update

An updated sos package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The sos package contains a set of tools that gather information from system hardware, logs and configuration files. The information can then be used for diagnostic purposes and debugging.

Bug Fix

BZ#748804

With the RHBA-2011-1028 advisory, the sosreport utility introduced the "--tmp-dir" command option allowing the sosreport tarballs to be stored in a user-specified directory. After this

change, sosreport no longer determined a directory for the tarballs from the TMP environment variable. The Red Hat Enterprise Virtualization 2.2. Log Collector application expected sosreport to use the TMP variable therefore Log Collector failed to collect the tarballs correctly from hosts. With this update, sosreport relies on the TMP environment variable again if the directory is not specified by the "--tmp-dir" option. Log Collector now works as expected.

All users of sos are advised to upgrade to this updated package, which fixes this bug.

4.182.2. RHSA-2012:0153 — Low: sos security, bug fix and enhancement update

An updated *sos* package that resolves one security issue, fixes several bugs, and adds various enhancements is now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The *sos* package contains a set of tools that gather information about system hardware and configuration.

Security Fixes

CVE-2011-4083

The sosreport utility incorrectly included Certificate-based Red Hat Network private entitlement keys in the resulting archive of debugging information. An attacker able to access the archive could use the keys to access Red Hat Network content available to the host. This issue did not affect users of Red Hat Network Classic.

Bug Fixes

BZ#733133

With the RHBA-2011-1028 advisory, the **sosreport** utility introduced the **`--tmp-dir`** command option allowing the sosreport tarballs to be stored in a user-specified directory. After this change, sosreport no longer determined a directory for the tarballs from the **`TMP`** environment variable. The **Red Hat Enterprise Virtualization 2.2 Log Collector** application expected sosreport to use the **`TMP`** variable therefore Log Collector failed to collect the tarballs correctly from hosts. With this update, sosreport relies on the **`TMP`** environment variable again if the directory is not specified by the **`--tmp-dir`** option and **Log Collector** now works as expected.

BZ#742567

Prior versions of the sos cluster module incorrectly used the python **`lstrip()`** method to extract the release number of the kernel package from the complete NVR (Name, Version, Release) string. This resulted in invalid release strings for certain kernel versions. As a result, **sos** incorrectly reported warnings for valid **`gfs2`** kernel module configurations. The cluster module has been modified to correctly obtain the release substring from the complete package NVR and false positives are no longer reported for valid package combinations.

BZ#717962

The internal API used by **sos** modules to collect files and directories handled symbolic links

with a relative target path incorrectly. Due to this bug only the symbolic links were copied to the sosreport tarball and the linked files were omitted. With this update, the file and directory copying routines have been modified to correctly copy and adjust symbolic link targets within the sosreport tree and targets of relative symbolic links are properly included in the generated report.

BZ#708346

Previously, **sosreport** used by default a threaded execution model to invoke plug-in modules. Consequently, a keyboard interrupt (**Ctrl**+**c**) failed to terminate the program due to improper synchronization between the main and child threads. The **sosreport** command now runs in single-threaded mode by default. This behavior was previously enabled by running the command with the **--no-multithread** option. This update adds the **--multithread** option to allow the previous behavior. As a result, sosreport now behaves more consistently when keyboard interrupts or other signals are received.

Note

Occasionally, sos can fail to respond to the keyboard interrupt (**Ctrl**+**C**). In such a case, the user is advised to suspend the process (press the **Ctrl**+**Z** keys in the interactive shell running sosreport) and kill the **sosreport** process: issue the **kill *pid*** commands where ***pid*** is the PID of the sosreport process. In the case the command fails, send the process the **SIGKILL** signal: issue the **kill -9 *pid*** command.

BZ#717167

Previously, **sos** attempted to determine whether the system is configured to use the traditional **syslogd** or **rsyslogd** daemon for logging. However, the used heuristic incorrectly identified an installed **rsyslog** as being used even though it was not configured. As a result, **sos** failed to collect custom-defined log destinations specified in the **syslog.conf** file of the host. The general module no longer attempts to determine, which log daemon is in use and collects any user-defined log destinations present in either the rsyslog or syslog configuration file.

BZ#716987

The **sosreport** command allows the user to restrict the maximum size of log files collected by the general plug-in using the **general.syslogsize** option. If the limit is exceeded, a portion of the log file is stored in the report in the plug-in sos_commands directory. Prior **sos** versions did not create a symbolic link from the default location for the size-limited log file to the location in the plug-in commands directory. If the user was unaware that log size limiting was applied, they may have assumed that the file was missing. With this release, **sosreport** creates symbolic links that point from the default location to the size-limited log file. Users can now find the expected content at the default location within sosreport regardless of the applied log file size limits.

BZ#655046

Due to an incorrect translation in the French locale files, **sos** printed the following confusing prompt when run in interactive mode:

```
Voulez vous continuer (y/n)?
```

Attempting to enter the suggested prompt response (**y**) resulted in an error. The expected response string has been changed to match the translated prompt and the program now suggests the correct response.

BZ#717480

Prior to this update, **sos** suppressed exceptions raised by plug-ins so that a bug in one plug-in would not prevent generation of the entire sosreport. Since plug-in exceptions are caught internally and not reported to the user or logged, this mechanism could conceal problems in the default plug-in set. The **sosreport** command has been modified to report any exceptions raised during plug-in processing to the sos log file or to the terminal output when run in verbose mode. Plug-in exceptions can now be discovered with the normal sos logging mechanisms while retaining the previous behavior of not permitting such exceptions to prematurely terminate the sos process.

BZ#750573

The **sosreport** command uses the Python libxml2 bindings to parse XML-formatted files such as **/etc/cluster/cluster.conf**. A malformed XML markup triggers a parser exception. This exception was caught by the generic module handling routines and was not reported to the user. Systems with a malformed **cluster.conf** reported no errors but the cluster module terminated abnormally without collecting the full set of data. The cluster module has been modified to catch parser exceptions internally and print a diagnostic message to alert the user to the problem.

Enhancements

BZ#565996

Veritas storage devices and high-availability products are commonly deployed on Red Hat Enterprise Linux systems, and provide scripts to collect configuration and status information for support purposes. Prior releases of sos were not able to include their output in sosreports. This update adds a new sos module, which collects output from Veritas scripts and Veritas support data is now collected automatically when sosreport is executed on qualified systems.

BZ#568635

Prior versions of sos did not collect the libvirt configuration or log files requiring administrators to manually collect and submit these files. A new sos module has been included and the libvirt configuration files in the **/etc/libvirt/** directory and log files in the **/var/log/libvirt/** directory are now collected when present.

BZ#667783

Prior to this update, **sos** did not support collection of gfs2-specific configuration and debugging information. A new sos module has been added that collects detailed configuration and debug information for this subsystem: file system metadata, dlm (distributed lock manager) state, journal sizes and counts, and gfs2 glock debugging data.

BZ#627416

The sos certificate system module did not support Red Hat Certificate System later than the 7.3 version. As a result, on Red Hat Certificate System 8.0 or later, the configuration and log files for these versions were not collected automatically. The **cs** module has now been updated to

include support for the later versions, and collection of configuration and log data on the later Red Hat Certificate System works as expected. In addition, the functionality of the **dogtag** module has been merged to the revised **cs** module and the **dogtag** module has been removed from the *sos* package.

BZ#641020

Prior versions of sos only collected basic configuration information for **Red Hat Enterprise MRG** components and the user of these components had to retrieve the required data manually. This update expands the set of data collected by the **mrggrid** module and sos now collects the full logs, configuration, and status information from MRG components automatically.

BZ#673246

Prior versions of sos did not capture InfiniBand-specific information. This update adds a new module to sos that captures this information and the **sosreport** command now automatically collects the output of the **ibv_devices** and **ibv_devinfo** commands on appropriately equipped systems.

BZ#677123

Systems using the software iSCSI target may require specific additional information to be collected in order to diagnose problems with these storage components. Prior versions of the *sos* package did not support collecting of this information and the user had to retrieve the details manually. This update adds the **iscsi** module that collects configuration and debugging output from the *scsi-target-utils* package and the information about configured software iSCSI targets is collected automatically.

All *sos* users are advised to upgrade to this updated package, which resolves the issue, fixes these bugs, and adds these enhancements.

4.183. spice-client

4.183.1. RHBA-2012:0147 — spice-client bug fix update

An updated spice-client package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The spice-client package provides the Simple Protocol for Independent Computing Environments (SPICE) client application. SPICE is a remote display protocol designed for virtual environments. SPICE users can access a virtualized desktop or server from the local system or any system with network access to the server. SPICE is used in Red Hat Enterprise Linux for viewing virtualized guests running on the KVM hypervisor or on Red Hat Enterprise Virtualization Hypervisors.

Bug Fix

BZ#790894

The SPICE client did not correctly handle an exception which was raised when trying to connect to a guest operating system with no running SPICE agent. Consequently, the SPICE client application terminated unexpectedly after the 30-second timeout. With this update, the SPICE client correctly handles this situation and successfully connects to the guest system without unnecessary waiting.

All users of spice-client are advised to upgrade to this updated package, which fixes this bug.

4.184. spice-usb-share

4.184.1. RHEA-2012:0174 — spice-usb-share enhancement update

An enhanced spice-usb-share package is now available for Red Hat Enterprise Linux 5.

The spice-usb-share package consists of non-free USB drivers which are used to share USB devices with a guest operating system connected via SPICE.

Enhancement

BZ#718816

The spice-usb-share package has been upgraded to version 4.9, which ensures that USB devices are shared correctly with SPICE client 0.8.1.

Users of spice-usb-share are advised to upgrade to this updated package, which adds this enhancement.

4.185. spice-xpi

4.185.1. RHBA-2012:0316 — spice-xpi bug fix and enhancement update

An updated spice-xpi package that fixes multiple bugs and adds multiple enhancements is now available for Red Hat Enterprise Linux 5.

The spice-xpi package provides the Simple Protocol for Independent Computing Environments (SPICE) extension for Mozilla that allows the SPICE client to be used from a web browser.

The spice-xpi package has been upgraded to upstream version 2.4, which provides a number of bug fixes and enhancements over the previous version.

Enhancement

BZ#612967

With this update, the SPICE XPI plug-in now allows the SPICE client to connect to both Red Hat Enterprise Linux 6 hosts and Red Hat Enterprise Linux 5 hosts.

All users of spice-xpi are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.186. squirrelmail

4.186.1. RHSA-2012:0103 — Moderate: squirrelmail security update

An updated squirrelmail package that fixes several security issues is now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are

available for each vulnerability from the CVE links associated with each description below.

SquirrelMail is a standards-based webmail package written in PHP.

Security Fixes

CVE-2011-2023

A cross-site scripting (XSS) flaw was found in the way SquirrelMail performed the sanitization of HTML style tag content. A remote attacker could use this flaw to send a specially-crafted Multipurpose Internet Mail Extensions (MIME) message that, when opened by a victim, would lead to arbitrary web script execution in the context of their SquirrelMail session.

CVE-2010-4555

Multiple cross-site scripting (XSS) flaws were found in SquirrelMail. A remote attacker could possibly use these flaws to execute arbitrary web script in the context of a victim's SquirrelMail session.

CVE-2011-2752

An input sanitization flaw was found in the way SquirrelMail handled the content of various HTML input fields. A remote attacker could use this flaw to alter user preference values via a newline character contained in the input for these fields.

CVE-2011-2753

It was found that the SquirrelMail Empty Trash and Index Order pages did not protect against Cross-Site Request Forgery (CSRF) attacks. If a remote attacker could trick a user, who was logged into SquirrelMail, into visiting a specially-crafted URL, the attacker could empty the victim's trash folder or alter the ordering of the columns on the message index page.

CVE-2010-4554

SquirrelMail was allowed to be loaded into an HTML sub-frame, allowing a remote attacker to perform a clickjacking attack against logged in users and possibly gain access to sensitive user data. With this update, the SquirrelMail main frame can only be loaded into the top most browser frame.

CVE-2010-2813

A flaw was found in the way SquirrelMail handled failed log in attempts. A user preference file was created when attempting to log in with a password containing an 8-bit character, even if the username was not valid. A remote attacker could use this flaw to eventually consume all hard disk space on the target SquirrelMail server.

CVE-2010-1637

A flaw was found in the SquirrelMail Mail Fetch plug-in. If an administrator enabled this plug-in, a SquirrelMail user could use this flaw to port scan the local network the server was on.

Users of SquirrelMail should upgrade to this updated package, which contains backported patches to correct these issues.

4.187. sssd

4.187.1. RHBA-2012:0164 — sssd bug fix and enhancement update

Updated *sssd* packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The *sssd* packages contain a set of daemons to manage access to remote directories and authentication mechanisms.

Bug Fixes

BZ#680443

Specifying a single server name in the **ipa_server** option in the **/etc/sssd/sssd.conf** file resulted in a successful dynamic update of the DNS records of the IPA DNS server. However, if two or more servers are specified, the update failed. This update addresses this issue, and specifying multiple servers in the **ipa_server** works as expected.

BZ#692455

When saving group memberships, **SSSD** uses a two-pass approach: save all the groups first, and then save their members. When a group GID is outside a specified range, the group should be skipped completely. Previously, **SSSD** correctly skipped the groups that were out of range during the save groups step, but then created the groups as a side effect of the save members step. As a result, **SSSD** did not filter groups which had a GID outside the specified range. With this update, the group save operation was changed so that only members of groups, which were processed successfully, are now saved, thus the bug is fixed.

BZ#694580

Previously, **SSSD** man pages only documented that some attributes expect lists of values but the man pages did not document how are these values supposed to be separated. With this update, the missing information has been added to the man pages, thus the bug is fixed.

BZ#698724

Previously, **SSSD** only informed the Kerberos library about the IP address of the password-change server if the password change request was delivered via the **pam_sss** module. As a result, tools that communicate directly with the password-change servers (for example **kpasswd**) were unable to operate. With this update, **SSSD** always passes the IP addresses of password change servers to the Kerberos library, thus the bug is fixed.

BZ#700168

Previously, the **simple** access provider in **SSSD** required that the user primary group was available to **SSSD**. As a result, the **simple** access provider did not work for users whose primary group was a local group stored in the **/etc/group** file because **SSSD** only handles remote groups. With this update, the failure to find the user primary group in the **simple** access provider is no longer treated as fatal so that users with the local primary group are handled correctly by the **simple** access provider.

BZ#707975

Previously, **SSSD** did not correctly escape certain special characters in the user names. As a

result, the **initgroups** and login operations failed for users whose user names contained special characters. With this update, the user names are now escaped, thus the bug is fixed.

BZ#707999

The IPA provider internally constructs an LDAP URI based on what the hostname that is specified by the ***ipa_server*** parameter resolves to. Previously, when the hostname resolved to an IPv6 address, the LDAP URI routines returned an error. As a result, the IPA provider was unable to function correctly in an IPv6 environment. With this update, the IPA provider now escapes all IPv6 addresses so that they can be consumed by the LDAP routines correctly, thus the bug is fixed.

BZ#708104

Previously, the Kerberos ticket renewal timer tasks were issued every time a back end detected the online state. This unintended behavior has been fixed in this update so that the ticket renewal tasks are now only issued as per the ***krb5_renew_interval*** parameter.

BZ#709352

Previously, the parameters for a domain name and user name were swapped in debug messages. With this update, the parameters have been fixed, thus the debug messages are now correct.

BZ#748818

The NSS responder process of **SSSD** uses an internal hash table. If the **SSSD** back end was restarted and the NSS responder reconnected, the hash table was iterated over, but elements in it were not checked for initialization. As a result, the NSS responder could have terminated unexpectedly after it was restarted due to accessing the already freed memory. With this update, all elements from the hash table are copied first and iterated over afterwards, thus the bug is fixed.

BZ#748820

SSSD stores all users and groups retrieved from the remote server in its local cache. When writing to this cache, transactions are used. If the RFC 2307bis schema was used, one transaction was used for each entity stored in the cache. As a result, the **initgroups** operation performed too many disk writes, thus slowing the operation down. With this update, all entities retrieved from the remote server are first stored in an internal hash table, and then only a single transaction is used to store all the groups and their memberships so that the **initgroups** operation is now faster, especially for users who are members of a large number of groups.

BZ#748822

Previously, **SSSD** required that all groups which **SSSD** worked with had a complete set of UNIX attributes, although the Active Directory groups can be individually set with or without the UNIX attributes. When a group without the UNIX attributes had a member with the UNIX attributes, **SSSD** did not recurse to the nested UNIX group. As a result, **SSSD** was unable to traverse the hierarchy correctly and the **initgroups()** operation did not return all groups correctly. With this update, **SSSD** has been changed so that it can examine non-UNIX groups for potential UNIX nested member groups. **SSSD** is now able to return the complete list of groups even if the hierarchy mixes UNIX and non-UNIX groups.

BZ#748833

Previously, **SSSD** incorrectly assumed that if the **ldap_default_authtok** option was used, the **ldap_default_authtok_type** option was set to **password** even if it was not explicitly specified in the configuration file. With this update, **password** has been made the default value for the **ldap_default_authtok_type** option, thus the bug is now fixed.

BZ#748834

Previously, the IPA provider reported an error if the provider did not find any group memberships for a user during the **initgroups** operation. As a result, the **initgroups** operation failed. With this update, the IPA provider has been fixed so that the provider now gracefully handles users without group memberships and the **initgroups** operation succeeds for users who are not members of any group.

BZ#748835

Previously, the internal resolver of **SSSD** was set to never retry other name servers, which were read from the **/etc/resolv.conf** file, if the first one failed to resolve a hostname. As a result, **SSSD** switched to offline mode without asking the other configured name servers. With this update, the bug has been fixed by configuring the resolver to query all name servers so that hostname resolution correctly retries until it either queries all the configured name servers or resolves the hostname.

BZ#748836

When the ***ldap_uri*** parameter was incorrectly configured so that the hostname part was missing, **SSSD** stored NULL in the pointer, in which the hostname was saved, and used it later on for establishing a connection. As a result, **SSSD** accessed the NULL pointer and terminated unexpectedly. With this update, the URI parsing function has been changed so it aborts when it cannot parse a valid hostname from the specified URI. **SSSD** reports an error and does not crash when an invalid ***ldap_uri*** parameter is used in the configuration file.

BZ#748842

Previously, the **SSSD** man page did not explicitly list the rules for encoding IPv6 addresses. The man page has been updated and the missing content added, thus the bug is fixed.

BZ#748844

Previously, the **sssd** daemon package did not explicitly specify that it required the *sssd-client* package of the same architecture. As a result, it was difficult to specify to install both primary and secondary architecture *sssd-client* packages on multiarch systems. With this update, the main *sssd* package now requires the *sssd-client* package of the same architecture, thus the bug is fixed.

BZ#748846

During the login process, **SSSD** could have attempted to create a **ccache** file for the user if the old **ccache** file had already expired. The SSH daemon used different processes with different UID values for different parts of the login process. As a result, if a user password expired after the user logged in, **SSSD** was unable to switch to a new **ccache**. With this update, **SSSD** forces removal of the old **ccache** if the Kerberos authentication subprocess returns a special **PAM_NEW_AUTHTOK_REQD** return code so that **SSSD** is able to recreate a

ccache file instead of an existing (but inactive) **ccache** file for a user who logs in via SSH with an expired password.

BZ#748847

Previously, **SSSD** relied on the **inotify** kernel subsystem to detect whether a Domain Name System (DNS) resolver file was changed. If **inotify** returned an error (for example due to resource exhaustion), **SSSD** terminated unexpectedly and network logins no longer worked. With this update, **SSSD** itself detects the failure in the described scenario and falls back to the five-second polling, fixing this bug.

BZ#748848

When **SSSD** communicated with an **OpenLDAP** server which supported server-side password policies but did not list them in the **supportedControl** attribute of the server **rootDSE** entry, **SSSD** terminated unexpectedly with a segmentation fault. With this update, this bug has been fixed.

BZ#748853

Previously, the buffer used for the dynamic DNS update operation was not big enough to contain IPv6 addresses. As a result, only part of the address was written into DNS, which corrupted the records. With this update, a larger buffer that is able to contain all address families is now used, thus the bug is fixed.

BZ#748855

Previously, **SSSD** did not properly close its Pluggable Authentication Modules (PAM) sockets after an authentication attempt, which eventually resulted in process resource exhaustion and a denial of service situation. With this update, **SSSD** has been modified to fix this problem, and file descriptors are now properly released when they are no longer in use.

BZ#748856

Previously, **SSSD** did not keep a copy of the list of supported LDAP controls during the whole LDAP operation. At the same time, it used the list of controls to determine if password expiration controls were available. As a result, password expiration warnings did not function properly because **SSSD** expected that they were not available. With this update, **SSSD** always requests the expiration controls so that the password expiration warnings are now displayed, as expected.

BZ#748857

Previously, certain Lightweight Directory Access Protocol (LDAP) deployments contained a group with the option **GID=0** set which acted like a "root" group. As a result, the operation that processed members belonging to the group with **GID=0** was aborted. With this update, groups with **GID=0** are treated as non-POSIX groups (that is groups that are containers only and not reported to clients) so that the groups are handled gracefully.

BZ#748858

After a connection was established to the server, **SSSD** never refreshed the resolved address and kept the old one until a failure occurred while communicating with the host. As a result, if a DNS record was changed, **SSSD** was not notified until the original address stopped working. With this update, the internal resolver has been switched to honor the time to live (TTL) values

that are read from DNS so that the resolved names are only valid for the period specified by the TTL field in DNS. The resolver refreshes the IP address after the interval passes.

BZ#748860

Previously, the LDAP provider man page incorrectly suggested that if the Generic Security Services Application Program Interface (GSSAPI) authentication is used and the Kerberos realm is not specified, the system default realm is used. With this update, the man page has been fixed so that it now correctly suggests that the realm configured in the **/etc/krb5.conf** file is used in the case mentioned above.

BZ#748864

Previously, **SSSD** checked for an incorrect DBus return code. As a result, instead of detecting timeouts properly, the monitor process disconnected from the back-end process, which resulted in failure to be notified about back end going online, and in network performance problems. With this update, **SSSD** checks for a correct DBus return code and improves handling of timeouts on the DBus connection, thus the mentioned problems are fixed.

BZ#748865

When processing group memberships for a user who was a member of a group that lacked any POSIX attributes, the loop index was incremented even for groups that were expected to be skipped. Instead of being skipped, groups without the POSIX attributes were returned with a random GID. With this update, the loop index is now only incremented for valid POSIX groups so that correct group membership is returned.

BZ#748866

Under certain circumstances, if the Simple Authentication and Security Layer (SASL) was used, libldap could have tried to canonicalize the hostname by doing a reverse lookup. As a result, the LDAP request could have been blocked. Also if the PTR record was wrong, **SSSD** was not able to authenticate to the server at all. With this update, the bug has been fixed by adding an **SSSD** configuration directive, which allows turning the canonicalization on or off. The canonicalization is off by default.

BZ#748869

Prior to this update, a generic and thus not understandable error message was displayed if a user password was changed but the password policy constraints were violated. With this update, the bug has been fixed by displaying the error message that clearly states what happened.

BZ#748873

During the password change, password policy attributes are checked in **SSSD**. If these attributes were incomplete, **SSSD** reported this password policy error as an internal error. As a result, the log message produced in this case was confusing. With this update, an authentication error is now reported and a proper log message is displayed so that the log messages related to the password policy are no longer confusing.

BZ#748874

SSSD uses an internal cache to store all entities retrieved from the server. Attributes of these entities can have different names in the cache and remote server. Under certain circumstances,

SSSD used the attribute names for the remote server instead of the names for the local cache. As a result, if non-default attribute names were used either for the group GID or name, all groups were processed and stored to the cache incorrectly, thus not returned to the NSS client. With this update, the cache attribute names are now correctly used when processing groups that are retrieved from the server, thus the bug is fixed.

BZ#748875

If a user or group entry had multiple names and none of them matched the Relative Distinguished Name (RDN) in LDAP, an error occurred during the processing of the entry in **SSSD**'s back end. As a result, entries with multiple names, with neither of them matching the RDN, were not stored and returned by **SSSD**. With this update, the entry that matches the RDN is now returned if the RDN attribute is the same as the name attribute, thus the bug is fixed.

BZ#748877

Previously, **SSSD** did not store alternative names in if the user or group included these alternative names. As a result, members of groups were not returned by **SSSD** if the **`member`** attribute had different value than what was determined as the primary name for that member object. With this update, **SSSD** stores all user name or group name aliases in the cache. When determining the membership structure, **SSSD** checks for aliases in addition to the primary name so that the membership structure is correctly determined and returned.

BZ#748878

Previously, **SSSD** did not store any alternative entry names if the name entry included the alternative entry names. As a result, entries with multiple names stored in the **SSSD** cache were not returned by **SSSD** to the NSS client if the entries were stored with different names than what the NSS client asked for. With this update, the bug has been fixed by storing name aliases in the cache in addition to the primary name.

BZ#748879

SSSD displayed a private LDAP error message because there were no special error messages available that were dedicated to error conditions indicated by the server-side password policies. As a result, a very generic, and thus not understandable error messages were printed when this error occurred. With this update, the bug has been fixed so that a clear and understandable error message is now printed when this error occurs.

BZ#748881

When converting string values returned by LDAP, **SSSD** used conversion with an implicit number base, which led to automatically detecting the base that was expected to be used. As a result, in case the UID or GID value returned from LDAP started with zero, the number was considered octal and after the conversion, a wrong value was used. With this update, explicit 10 base is now used for conversion so that the UID and GID values are not erroneously converted anymore.

BZ#748882

Previously, the example configuration file shipped with the **SSSD** contained directives, which were inaccurate, outdated, and technically inappropriate. With this update, a new example configuration file is provided, thus the bug is fixed.

BZ#748895

The Name Service Switch (NSS) responder process of **SSSD** uses an internal hash table. If **SSSD** back end was restarted and the NSS responder reconnected, the hash table was accessed but not checked for existence. As a result, under certain circumstances, nothing was stored in the hash table before the NSS responder reconnected, and the NSS responder accessed uninitialized memory and terminated unexpectedly. With this update, the hash table is now checked for existence, thus the bug is fixed.

BZ#748896

Previously, if internal communication between the PAM responder and one of **SSSD**'s back ends timed out, a handling routine was invoked. Under certain circumstances, this routine could have caused a race condition which could have resulted in accessing memory that has been freed. As a result, the PAM responder terminated unexpectedly. With this update, timeout handling routine does not free the context until all operations on this context are done, thus the bug is fixed.

BZ#748898

SSSD's components communicate using the DBus protocol. On initializing the DBus server, the DBus library is given a file name that represents a known interface. DBus creates the socket on server startup. When server shuts down, it calls a DBus cleanup function which removes the socket. If one of the components was restarted, a race condition could have caused the socket to be removed by the old component instance after the new instance was already running and connected to it. With this update, path names that contain the server process' PID are passed to DBus and a symbolic link with a known and defined path name is pointed to the path name with PID. Clients connect to the well-known symbolic link paths. When the DBus server exits, the server only removes the path name appended with PID. Clients are still connected to the same path no matter what server is the symbolic link pointed to.

BZ#748899

Prior to this update, the HBAC provider was performing case-sensitive matches on hostnames. However, hostnames, as defined by RFC 952, are case insensitive. This update modifies the hostname matching code to be case insensitive.

BZ#758163

When establishing a connection to an LDAP server, **SSSD** did not handle all possible error codes it could receive but only the ETIMEDOUT error code. Therefore, if **SSSD** received an error code different from ETIMEDOUT, it did not perform the expected failover to another LDAP server and switched to off-line mode. With this update, **SSSD** has been modified to handle all error codes received on connection attempt. **SSSD** now tries to connect to all specified LDAP servers and goes off-line only when it fails to connect to all of them.

BZ#758168

SSSD responders did not verify whether a username string, which was passed to **SSSD** by a client application, contained any invalid UTF-8 characters. As a consequence, **SSSD** terminated unexpectedly when trying to pass such a string to the data provider over the D-Bus protocol, and the validation test performed by the **libdbus** library failed. To prevent this problem from occurring, UTF-8 validity checks on the string have been added in the underlying **SSSD** code. **SSSD** now does not accept username strings that are not compliant with UTF-8 encoding so that **SSSD** no longer crashes.

BZ#760166

Previously, the host-based access control part of **SSSD** treated all its attributes as plain strings. As a result, case-insensitive comparisons of attributes (for example host group names) failed if the attributes contained UTF-8 characters. With this update, the **SSSD** host-based access control provider utilizes **`libunistring`** for performing string comparisons where applicable so that **SSSD** is able to handle UTF-8 strings in the host-based access control rules.

Enhancements

Note

For more information on the most important of the Red Hat Enterprise Linux 5.8 SSSD enhancements, refer to the Red Hat Enterprise Linux 5.8 Release Notes.

BZ#773327

SSSD now logs the full dynamic DNS message into the debug logs. The message contains the following data:

- hostname of the client,
- IP addresses of clients' network interface (either the one the client uses to connect to LDAP or one selected in the SSSD configuration file),
- client DNS zone,
- Kerberos realm of the client,
- IPA server hostname.

BZ#748854

With this update, a new option **`ipa_hbac_treat_deny_as`** has been added to **SSSD**. The default value for the option is **`DENY_ALL`**, which means that any **`DENY`** rule in the whole set of rules will deny access regardless of what is the actual rule. Alternatively, the option can be set to **`IGNORE`** to skip the **`DENY`** rules.

Important

By ignoring the **`DENY`** rules altogether, setting the **`ipa_hbac_treat_deny_as`** option to **`IGNORE`** may, under certain circumstances, allow access to users who are not intended to be allowed.

BZ#748867

Previously, **SSSD** did not set a special path for the Kerberos replay cache files. As a result, the files were stored in the **`/var/tmp/`** directory. Because the file names are not standardized, they were not handled by the Security-Enhanced Linux (SELinux) policy correctly. As a result, when using SELinux in Enforcing mode, **SSSD** did not work with the option **`krb5_validate`** set to **`true`**. With this update, support to specify the Kerberos replay cache directory, both at compilation time and in the configuration file, has been added into **SSSD**, also a corresponding

SELinux policy update has been made to accommodate the Kerberos replay cache directory, thus the bug is fixed.

All users of SSSD should upgrade to these updated packages, which fix these bugs and add this enhancement.

4.188. subscription-manager

4.188.1. RHBA-2012:0148 — subscription-manager bug fix update

Updated subscription-manager packages that fix three bugs are now available for Red Hat Enterprise Linux 5.

The subscription-manager package provides programs and libraries to allow users to manage subscriptions and yum repositories from the Red Hat Entitlement platform.

Bug Fix

BZ#788661

On Red Hat Enterprise Linux 5, subscription management does not support software channels for 64-bit PowerPC architectures. Therefore, the "install-num-migrate-to-rhsm" utility did not work on these architectures, and users were not able to migrate their systems to Certificate-based Red Hat Network (RHN). With this update, the "install-num-migrate-to-rhsm" utility has been modified to use the supported PowerPC product certificates instead. Systems installed on 64-bit PowerPC architectures can now be migrated properly from Classic RHN to Certificate-based RHN.

BZ#788665

Previously, the "rhn-migrate-classic-to-rhsm" utility did not handle correctly when an Red Hat Network (RHN) software channel supported more than one product. Consequently, the utility installed superfluous product certificates when client systems were subscribed to particular RHN channels. This update corrects "rhn-migrate-classic-to-rhsm" so that only the proper product certificate is now installed under these circumstances.

BZ#790437

Previously, the "install-num-migrate-to-rhsm" utility did not work correctly for certain products. Consequently, the utility installed also a superfluous Desktop product certificate when the system was provided with an installation number for a Workstation product and vice versa. With this update, "install-num-migrate-to-rhsm" has been fixed and only the correct product certificate is now installed under these circumstances.

All users of subscription-manager are advised to upgrade to these updated packages, which fix these bugs.

4.188.2. RHBA-2012:0154 — subscription-manager bug fix and enhancement update

Updated *subscription-manager* packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The **Subscription Manager** tool allows users to understand the specific products which have been installed on their machines, and the specific subscriptions which their machines are consuming.

Bug Fixes

BZ#772921

When executing the **subscription-manager-gui** tool, an icon in the notification area displayed the following message if the entitlement certificate had expired:

```
Invalid or Missing Entitlement certificates
```

If the user clicked on the icon, the window of **subscription-manager-gui** was closed and the application terminated unexpectedly. This was because a new instance of the application was started by clicking on the icon. The second instance considered the first instance to be running, sent it a **DBus** message to raise the window to the foreground and so caused the crash. With this update, a second instance of **subscription-manager-gui** is not started in the aforementioned scenario, which prevents the utility from crashing.

BZ#782549

When executing the **subscription-manager-gui** tool on systems with an expired entitlement certificate, the tool, in certain cases, failed to start and a traceback error occurred. With this update, subscription-manager-gui starts successfully with an expired entitlement certificate. The certificate can be viewed on the **My Installed Software** tab.

BZ#719548

The **subscription-manager-gui** utility did not specify explicit dependency on the *dbus-x11* package. As a consequence, subscription-manager-gui failed to start when attempting to start subscription-manager-gui remotely on a 64-bit Itanium system by using the **Xvnc** application. The *dbus-x11* package has been included as a prerequisite for the *subscription-manager-gnome* package in the spec file, and is be installed along with the *subscription-manager* packages. The subscription-manager-gui application now runs as expected in the described scenario.

BZ#738517

Previously, the yum utility issued an **HTTPS GET** request instead of an **HTTPS CONNECT** request. As a consequence, retrieving content from the content delivery network (CDN) by using an HTTP proxy failed. With this update, if the user uses **https://** instead of **http://** for the proxy URL, an HTTPS CONNECT request is made to the proxy instead of an invalid HTTPS GET request. Users are now able to register properly and retrieve the content.

BZ#732509

Previously, users were not able to import a certificate by using the command line interface (CLI). This update adds the new CLI **import** option, and the root user can now successfully import a certificate.

Enhancements

BZ#766895

This update introduces the **hypervisorCheckIn()** call that allows sending mapping of the

host or guest IDs for creating or updating an account.

BZ#734480

This update adds configuration that allows Red Hat Enterprise Virtualization Hypervisor to register with Subscription Asset Manager (SAM).

BZ#726407

This update adds a new tool to migrate Red Hat Network Classic users to the certificate-based Red Hat Network.

BZ#726409, 741974

This update adds support for stacking of entitlements. This allows users to combine a set of subscriptions on a single machine in order to become compliant. For example, 2-socket (socket pair) subscriptions can now be combined to cover a four-socket machine, and 4-guest subscriptions can be combined in order to allow eight guests on a machine.

BZ#726411

Previously, if a subscription had expired, users had to log into each machine and attempt to locate new subscriptions. This update adds support for certificate healing, which allows machines (if required) to automatically look for new subscriptions after the previous subscription has expired.

BZ#643973

This update adds support of activation keys with encrypted credentials. The keys are used by a script when the user makes use of the subscription-manager utility to register with Subscription Asset Manager. This prevents from disclosing secure information.

All users of *subscription-manager* are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.189. sudo

4.189.1. RHSA-2012:0309 — Low: sudo security and bug fix update

An updated sudo package that fixes one security issue and various bugs is now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The sudo (superuser do) utility allows system administrators to give certain users the ability to run commands as root.

Security Fix

CVE-2011-0010

A flaw was found in the sudo password checking logic. In configurations where the sudoers

settings allowed a user to run a command using sudo with only the group ID changed, sudo failed to prompt for the user's password before running the specified command with the elevated group privileges.

Bug Fixes

BZ#673072

A NULL pointer dereference bug caused the sudo utility to terminate unexpectedly with a segmentation fault. This happened if the utility was run with the -g option and configured not to demand the password from the user who ran the sudo utility. With this update, the code has been modified and the problem no longer occurs.

BZ#617061

The sudo utility failed to load sudoers from an LDAP (Lightweight Directory Access Protocol) server after the sudo tool was upgraded. This happened because the upgraded nsswitch.conf file did not contain the instruction to search for sudoers on the LDAP server. This update adds the lost instruction to /etc/nsswitch.conf and the system searches for sources of sudoers on the local file system and then on LDAP, if applicable.

BZ#627543

The sudo tool interpreted a Runas alias specifying a group incorrectly as a user alias and the alias seemed to be ignored. With this update, the code for interpreting such aliases has been modified and the Runas group aliases are honored as expected.

BZ#750318

Prior to this update, sudo did not parse comment characters (#) in the ldap.conf file correctly and could fail to work. With this update, parsing of the LDAP configuration file has been modified and the comment characters are parsed correctly.

BZ#697111

The sudo utility formats its output to fit the width of the terminal window. However, this behavior is undesirable if the output is redirected through a pipeline. With this update, the output formatting is not applied in the scenario described.

BZ#477185

Previously, the sudo utility performed Security-Enhanced Linux (SELinux) related initialization after switching to an unprivileged user. This prevented the correct setup of the SELinux environment before executing the specified command and could potentially cause an access denial. The bug has been fixed by backporting the SELinux related code and the execution model from a newer version of sudo.

BZ#673157

On execv(3) function failure, the sudo tool executed an auditing call before reporting the failure. The call reset the error state and, consequently, the tool incorrectly reported that the command succeeded. With this update, the code has been modified and the problem no longer occurs.

All users of sudo are advised to upgrade to this updated package, which resolves these issues.

4.190. syslinux

4.190.1. RHBA-2012:0207 — syslinux bug fix update

Updated syslinux packages that fix a bug are now available for Red Hat Enterprise Linux 5.

The syslinux utility is responsible for booting the operating system kernel.

Bug Fix

BZ#500631

Although the syslinux package contains ELF objects, the debuginfo package was previously empty. This bug has been fixed and the syslinux-debuginfo package now contains debugging information as expected.

Users of syslinux are advised to upgrade to these updated packages, which fix this bug.

4.191. system-config-bind

4.191.1. RHBA-2011:1505 — system-config-bind bug fix update

An updated system-config-bind package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The system-config-bind package provides a graphical user interface (GUI) to configure the Berkeley Internet Name Domain (BIND) Domain Name System (DNS) server.

This updated system-config-bind package includes fixes for the following bugs:

BZ#511864

Prior to this update the system-config-bind utility no longer parsed include statements within a view clause. Consequently zones in a config file referenced by an include statement within a view clause were not shown. With this update include statements are correctly parsed and zones referenced in this way are once again shown.

BZ#462846

When configuring a name server (NS) record for a domain, if an invalid name was given in the Server Domain Name field a modal dialog box would display, "Bad DNS Name:", and clicking "OK" did not allow a valid name to be entered. Consequently it was not possible to correct the mistake. With this update the dialog box now correctly responds to clicking "OK" and a correct Server Domain Name can be entered.

All users of system-config-bind are advised to upgrade to this updated package, which fixes these bugs.

4.192. system-config-cluster

4.192.1. RHBA-2012:0210 — system-config-cluster bug fix and enhancement update

An updated system-config-cluster package that fixes one bug and adds one enhancement is now available for Red Hat Enterprise Linux 5.

The system-config-cluster package contains a utility that allows the management of cluster configuration in a graphical setting.

Bug Fix

BZ#719658

The system-config-cluster utility configured MySQL resources with an invalid attribute, "mysql_options". Consequently, a cluster configuration file failed a validation check if the cluster configuration contained MySQL resources. With this update, system-config-cluster correctly defines the MySQL resources with the "mysqld_options" attribute and thus provides valid cluster configuration.

Enhancement

BZ#532761

The system-config-cluster utility lacked the ability to configure resources for an Oracle database. This update adds the necessary support, and system-config-cluster now allows to create and configure Oracle resources.

All users of system-config-cluster are advised to upgrade to this updated package, which fixes this bug and adds this enhancement.

4.193. system-config-date

4.193.1. RHBA-2011:1490 — system-config-date bug fix update

An updated system-config-date package that fixes a bug is now available for Red Hat Enterprise Linux 5.

system-config-date is a graphical interface for changing the system date and time, configuring the system time zone, and setting up the NTP daemon to synchronize the time of the system with an NTP time server.

Bug Fix

BZ#529071

Prior to this update, the system-config-date program set date and time in two separate steps which sometimes caused time update threads in Xen virtual machines (VMs) to become unresponsive. This version sets date and time together in one step. As a result, any Xen VMs running on the host no longer hang during the date and time update process.

All users of system-config-date are advised to upgrade to this updated package, which fixes this bug.

4.194. system-config-display,

4.194.1. RHBA-2012:0285 — system-config-display, rhpxl, and pyxf86config bug fix update

Updated system-config-display, rhpxl, and pyxf86config packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The system-config-display package contains a tool for configuring the xorg.conf file that is used by the X Window System for display configuration. The rhpxl package contains a Python library for configuring and running the X Window System. The pyxf86config package contains a Python binding to the C-language parser for the X Window System's xorg.conf file.

Bug Fixes

BZ#429949, BZ#750352

Prior to this update, running the system-config-display utility with the "--set-hsync" and "--set-vsync" command line options or setting these options in a kickstart file for Anaconda failed to create a "Monitor" section in the xorg.conf file. This update corrects this error so that the system-config-display utility now creates this section as expected.

BZ#430579

The previous version of the system-config-display utility allowed the user to configure dual head mode regardless of the driver in use. Consequent to this, enabling dual head mode on a system with a video driver that does not support this feature (such as "nv") caused system-config-display to create a non-working configuration file. With this update, the utility has been adapted to disable dual head mode when such a driver is detected.

BZ#755542

Previously, an incomplete dual head configuration could cause the system-config-display utility to terminate unexpectedly with a traceback. This update adapts the underlying source code to make sure that such an error no longer occurs.

All users of system-config-display, rhpxl, and pyxf86config are advised to upgrade to these updated packages, which fix these bugs.

4.195. system-config-network

4.195.1. RHBA-2012:0231 — system-config-network bug fix and enhancement update

Updated system-config-network packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 5.

System-config-network is the user interface of the network configuration tool, supporting Ethernet, Wireless, TokenRing, ADSL, ISDN and PPP.

These updated system-config-network packages provide fixes for the following bugs:

BZ#501530

Previously, when a file "/etc/sysconfig/network-scripts/route-eth[X]" contained static route options that system-config-network did not parse, that file was removed upon editing eth[X] in system-config-network even if the static route options had not been changed. This update

corrects the issue such that system-config-network no longer removes route-eth[X] files in the described scenario.

BZ#504824

Previously, if the configuration for a bonded interface slave device was edited, and the "Bind to MAC address" option was selected, it took the MAC address from the master interface. Consequently, it broke the bond configuration. With this update, system-config-network now prevents the user from corrupting the bond configuration by disabling the "Bind to MAC address" option on bonded slave devices.

BZ#522618

The system-config-network tool provided support for QDIO Ethernet (QETH) devices on IBM S/390 but did not provide online help. With this update, the "Establishing a QETH Connection" chapter has been added to Help.

BZ#523493

When adding a new QETH device, system-config-network gave unnecessary warnings despite completing successfully. With this update, the warnings that were appearing when adding new QETH device have been removed.

BZ#538749

Previously, system-config-network could show an incorrect relationship between hardware and the interface name on some hardware. The issue was resolved by migrating the backend from kudzu to the Hardware Abstraction Layer (HAL).

BZ#602688

Previously, if GATEWAYDEV was set in "/etc/sysconfig/network", system-config-network removed the option without notice. With this update, a patch has been applied and the problem no longer occurs.

BZ#701322

Previously, when editing an alias device interface with the system-config-network tool, the Device Alias Number always showed 0 when the tool was restarted. The problem has been fixed and the Device Alias Number now shows the correct value.

Enhancement

BZ#663682

With this update, support for LAN channel station (LCS) devices has been added to system-config-network.

Users are advised to upgrade to these updated system-config-network packages, which fix these bugs and add this enhancement.

4.196. system-config-printer

4.196.1. RHSA-2011:1196 — Moderate: system-config-printer security update

Updated system-config-printer packages that fix one security issue are now available for Red Hat Enterprise Linux 4 and 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

system-config-printer is a print queue configuration tool with a graphical user interface.

Security Fix

CVE-2011-2899

It was found that system-config-printer did not properly sanitize NetBIOS and workgroup names when searching for network printers. A remote attacker could use this flaw to execute arbitrary code with the privileges of the user running system-config-printer.

All users of system-config-printer are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. Running instances of system-config-printer must be restarted for this update to take effect.

4.197. system-switch-mail

4.197.1. RHBA-2011:1489 — system-switch-mail bug fix update

Updated system-switch-mail packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The system-switch-mail utility is the Mail Transport Agent Switcher. It enables users to easily switch between various mail transport agents.

Bug Fix

BZ#521904

Prior to this update system-switch-mail contained the shebang line, "#!/usr/bin/env python". This made it difficult to install alternative versions of Python on the system. With this update the shebang lines in Python executables have been changed to, "#!/usr/bin/python", to ensure the Python interpreter installed on the system is used.

All users of system-switch-mail are advised to upgrade to these updated packages, which resolve this issue.

4.198. systemtap

4.198.1. RHSA-2011:1089 — Moderate: systemtap security update

Updated systemtap packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is

available from the CVE link associated with the description below.

SystemTap is an instrumentation system for systems running the Linux kernel. The system allows developers to write scripts to collect data on the operation of the system.

Security Fix

CVE-2011-2503

A race condition flaw was found in the way the staprun utility performed module loading. A local user who is a member of the stapusr group could use this flaw to modify a signed module while it is being loaded, allowing them to escalate their privileges.

SystemTap users should upgrade to these updated packages, which contain a backported patch to correct this issue.

4.198.2. RHBA-2012:0200 — systemtap bug fix update

Updated systemtap packages that fix various bugs are now available for Red Hat Enterprise Linux 5.

SystemTap provides infrastructure to simplify the gathering of information about the running Linux system. This assists diagnosis of a performance or a functional problem. Developers can write scripts to collect data without the need to go through the tedious and disruptive instrument, recompile, install, and reboot sequence that may be otherwise required to collect data.

The systemtap package has been upgraded to upstream version 1.6, which provides a number of bug fixes and enhancements over the previous version. (BZ#683481)

Bug Fixes

BZ#718678

When running the "with server" portion of the SystemTap buildok test suite, the server needs an authorized certificate for signing the code the compiler server built. In some cases, a client running the test suite never obtained the authorized certificate. Consequently, additional failures were reported by the test suite compared to the self-hosted buildok test runs. This bug has been fixed and now, results for the "with server" portion of test suite and the self-hosted test suite match.

BZ#709190

The systemtap data structure to track address accesses requires a locking mechanism to prevent data corruption. Previously, spinlocks were used but they caused kernel panics if excessive contention for reading the data structure occurred. With this update, the locking mechanism has been changed to rwlock, which allows concurrent reading of the data structure, thus fixing this bug.

BZ#711976

For some error conditions (such as "out of memory"), the debugfs directory associated with a systemtap script remained in the system even after the script exited. Consequently, other scripts run afterwards were unable to create their own debugfs directory until the system had been rebooted. With this update, the runtime transport code has been updated to remove debugfs directories every time a systemtap script exits.

BZ#706185

Previously, tracepoint names for softirq probe points (used in older kernels) and for the irq.stp tapset (used in newer kernels) did not match. Consequently, the softirq.* probe points were not found on kernels in Red Hat Enterprise Linux 5. Now, the irq.stp tapset has been updated to allow systemtap to find older softirq probe points in older kernels.

BZ#757118

In some cases, the operands in the newest version of user-space markers could not be parsed, causing some tests to fail. With this update, SystemTap parsing of marker arguments has been fixed to handle the operands for the newest version of user-space markers and the tests now pass as expected.

BZ#757723

The memory-write_shared_copy.stp test uses the memory.stp tapset's vm.write_shared_copy probe. In earlier versions of systemtap, this probe was a dummy, letting the test case falsely pass. In later versions, it became a real probe, but due to incomplete debug information generated by the gcc compiler, it cannot be fully resolved on a Red Hat Enterprise Linux 5 kernel. Consequently, the test case fails. This appeared as a regression, because the earlier pass of the test was in fact false. With this update, this test case has been designated as a "KFAIL" (known failure) and is no longer considered a regression.

Users of systemtap are advised to upgrade to these updated packages, which fix these bugs.

4.199. tog-pegasus

4.199.1. RHBA-2012:0257 — tog-pegasus bug fix update

Updated tog-pegasus packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The tog-pegasus packages provide OpenPegasus Web-Based Enterprise Management (WBEM) services for Linux. WBEM enables management solutions that deliver increased control of enterprise resources. WBEM is a platform and resource independent Distributed Management Task Force (DMTF) standard that defines a common information model (CIM) and communication protocol for monitoring and controlling resources from diverse sources.

The tog-pegasus packages have been upgraded to upstream version 2.11.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#713972)

Bug Fixes

BZ#544053

Previously, when the CMPIArray variable type was cloned, each array element was cloned by calling the respective clone function of the CMPIType variable type. When attempting to release the cloned CMPIArray, none of the array elements was released by calling their respective release functions. This resulted in a memory leak. This update introduces a new boolean flag which handles releasing of the cloned CMPIArray variable type.

BZ#553123

The OpenPegasus init script contains the "condrestart" action. However, the "condrestart" option was missing in the help strings, and this option was not displayed. With this update, help

strings are complete and the "condrestart" option is correctly displayed.

Enhancement

BZ#713987

This update adds the Privilege Separation option to provide support for the IBM Systems Director suite.

All users of tog-pegasus are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.200. tomcat5

4.200.1. RHSA-2011:1845 — Moderate: tomcat5 security update

Updated tomcat5 packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages (JSP) technologies.

Security Fixes

CVE-2010-3718

It was found that web applications could modify the location of the Tomcat host's work directory. As web applications deployed on Tomcat have read and write access to this directory, a malicious web application could use this flaw to trick Tomcat into giving it read and write access to an arbitrary directory on the file system.

CVE-2011-0013

A cross-site scripting (XSS) flaw was found in the Manager application, used for managing web applications on Apache Tomcat. A malicious web application could use this flaw to conduct an XSS attack, leading to arbitrary web script execution with the privileges of victims who are logged into and viewing Manager application web pages.

CVE-2011-1184

Multiple flaws were found in the way Tomcat handled HTTP DIGEST authentication. These flaws weakened the Tomcat HTTP DIGEST authentication implementation, subjecting it to some of the weaknesses of HTTP BASIC authentication, for example, allowing remote attackers to perform session replay attacks.

CVE-2011-2204

A flaw was found in the Tomcat MemoryUserDatabase. If a runtime exception occurred when creating a new user with a JMX client, that user's password was logged to Tomcat log files. Note: By default, only administrators have access to such log files.

Users of Tomcat should upgrade to these updated packages, which contain backported patches to correct these issues. Tomcat must be restarted for this update to take effect.

4.201. udev

4.201.1. RHBA-2011:1448 — udev bug fix update

Updated udev packages that resolve one bug are now available for Red Hat Enterprise Linux 5.

The udev packages implement a dynamic device-directory, providing only the devices present on the system. This dynamic directory runs in user space, dynamically creates and removes devices, provides consistent naming, and a user space API. The udev device manager replaces the devfs device file system, providing greater hot plug functionality.

Bug Fix

BZ#736475

On a system boot, the udev helper application, pam_console_apply, was called for every disk that appeared on the system. This was unnecessary for example for SCSI disks, which do not have set default pam console permissions. As a consequence, the boot process was significantly slowed down if a system contained a large number of disks. To fix this problem, the /etc/udev/rules.d/95-pam-console.rules file has been marked as a configuration file and it will not be automatically updated with newer udev versions. System administrators should now comment out the pam_console_apply call in this file on systems that do not need a normal console user access to devices.

All users of udev are advised to upgrade to these updated packages, which fix this bug.

4.202. unixODBC

4.202.1. RHEA-2012:0226 — unixODBC enhancement update

Updated unixODBC packages that add one enhancement are now available for Red Hat Enterprise Linux 5.

The unixODBC packages contain a library for programs that use the ODBC standard to connect to database servers.

Enhancement

BZ#497016

This update divides the unixODBC package into a main package and a unixODBC-libs sub-package. The main package now contains only command-line utility programs (isql and others), while unixODBC-libs contains all the library files that are needed by other applications. The unixODBC-devel and unixODBC-kde sub-packages remain as they were. This split allows unixODBC-libs to be installed concurrently with unixODBC64-libs from the newer unixODBC64 package set, thus allowing applications that use either version of the ODBC API to be supported at the same time. With this update, unixODBC-libs can be installed concurrently with unixODBC64-libs from the newer unixODBC64 package set and applications that use either version of the ODBC API can be used concurrently.

All users of unixODBC are advised to upgrade to these updated packages, which add this enhancement.

4.203. util-linux

4.203.1. RHSA-2012:0307 — Low: util-linux security, bug fix, and enhancement update

An updated util-linux package that fixes multiple security issues, various bugs, and adds two enhancements is now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The util-linux package contains a large variety of low-level system utilities that are necessary for a Linux system to function. Among others, util-linux contains the fdisk configuration tool and the login program.

Security Fix

CVE-2011-1675, **CVE-2011-1677**

Multiple flaws were found in the way the mount and umount commands performed mtab (mounted file systems table) file updates. A local, unprivileged user allowed to mount or unmount file systems could use these flaws to corrupt the mtab file and create a stale lock file, preventing other users from mounting and unmounting file systems.

Bug Fixes

BZ#646300

When the user logged into a telnet server, the login utility did not update the utmp database properly if the utility was executed from the telnetd daemon. This was due to telnetd not creating an appropriate entry in a utmp file before executing login. With this update, correct entries are created and the database is updated properly.

BZ#650937

Various options were not described on the blockdev(8) manual page. With this update, the blockdev(8) manual page includes all the relevant options.

BZ#677452

Prior to this update, the build process of the util-linux package failed in the po directory with the following error message: "@MKINSTALLDIRS@: No such file or directory". An upstream patch has been applied to address this issue, and the util-linux package now builds successfully.

BZ#678407

Previously, the ipcs(1) and ipcrm(1) manual pages mentioned an invalid option, "-b". With this update, only valid options are listed on those manual pages.

BZ#699639

Previously, the mount(8) manual page contained incomplete information about the ext4 and XFS file systems. With this update, the mount(8) manual page contains the missing information.

Enhancements

BZ#678430

Previously, if DOS mode was enabled on a device, the fdisk utility could report error messages similar to the following:

```
Partition 1 has different physical/logical beginnings (non-Linux?):
phys=(0, 1, 1) logical=(0, 2, 7)
```

This update enables users to switch off DOS compatible mode (by specifying the "-c" option), and such error messages are no longer displayed.

BZ#726572

This update adds the "fsfreeze" command which halts access to a file system on a disk.

All users of util-linux are advised to upgrade to this updated package, which contains backported patches to correct these issues and add these enhancements.

4.204. virt-manager

4.204.1. RHBA-2012:0216 — virt-manager bug fix update

An updated virt-manager package that fixes multiple bugs is now available for Red Hat Enterprise Linux 5.

Virtual Machine Manager (virt-manager) is a graphical tool for administering virtual machines for KVM, Xen, and QEMU. The virt-manager utility can start, stop, add or remove virtualized devices, connect to a graphical or serial console, and see resource usage statistics for existing virtualized guests on local or remote machines. It uses the libvirt API (Application Programming Interface).

Bug Fixes

BZ#589436

Previously, when executing the virt-manager utility on guests that used the KDE environment and X11 forwarding, the application window was displayed only for a short moment and terminated immediately afterwards. This update removes unnecessary hide_all() calls, and the window now remains open as expected.

BZ#701873

Previously, when the user created a disk image guest, and attached a Small Computer System Interface (SCSI) disk image for the storage, this addition damaged the guest disk image, which was no longer able to boot. This update disables the SCSI option for QEMU connections, and so prevents guest disk images from being damaged.

BZ#708178

Previously, the "env" command was used to provide the path to the python binary in the virt-manager script. This could in certain cases cause the virt-manager utility to misbehave. This update explicitly specifies the python binary path, and so ensures correct behavior of virt-

manager.

BZ#712206

Previously, on the Xen hypervisor, the virt-manager utility did not use the specified disk size when using the keyboard for navigation. As a consequence, insufficient space could prevent a guest operating system from being installed. This update modifies virt-manager to use the specified disk size correctly when navigating by keyboard. Guest operating systems can now be installed successfully.

All users of virt-manager are advised to upgrade to this updated package, which fixes these bugs.

4.205. virtio-win

4.205.1. RHBA-2011:1288 — virtio-win floppy disk update

Spice QXL drivers have been added to the virtio-win RPM package.

To enable simple installation and updating of drivers without requiring an MSI installer to be run, Spice QXL drivers have been added to the virtio-win RPM package.

4.206. Virtualization_Guide

4.206.1. RHBA-2012:0177 — Virtualization_Guide bug fix and enhancement update

Updated Virtualization packages that fix numerous bugs and add several enhancements are now available for Red Hat Enterprise Linux 5.

The Virtualization Guide documents relevant information regarding the installation, configuration, administration, and troubleshooting of virtualization technologies in Red Hat Enterprise Linux 5.

The Virtualization Guide has been updated to version 5.8, which provides a number of bug fixes and enhancements over the previous version. (BZ#727334)

All users of the Virtualization Guide are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.207. vixie-cron

4.207.1. RHSA-2012:0304 — Low: vixie-cron security, bug fix, and enhancement update

An updated vixie-cron package that fixes one security issue, several bugs, and adds one enhancement is now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The vixie-cron package contains the Vixie version of cron. Cron is a standard UNIX daemon that runs

specified programs at scheduled times. The vixie-cron package adds improved security and more powerful configuration options to the standard version of cron.

Security Fix

CVE-2010-0424

A race condition was found in the way the crontab program performed file time stamp updates on a temporary file created when editing a user crontab file. A local attacker could use this flaw to change the modification time of arbitrary system files via a symbolic link attack.

Red Hat would like to thank Dan Rosenberg for reporting this issue.

Bug Fixes

BZ#455664

Cron jobs of users with home directories mounted on a Lightweight Directory Access Protocol (LDAP) server or Network File System (NFS) were often refused because jobs were marked as orphaned (typically due to a temporary NSS lookup failure, when NIS and LDAP servers were unreachable). With this update, a database of orphans is created, and cron jobs are performed as expected.

BZ#460070

Previously, cron did not log any errors if a cron job file located in the /etc/cron.d/ directory contained invalid entries. An upstream patch has been applied to address this problem and invalid entries in the cron job files now produce warning messages.

BZ#476972

Previously, the "@reboot" crontab macro incorrectly ran jobs when the crond daemon was restarted. If the user used the macro on multiple machines, all entries with the "@reboot" option were executed every time the crond daemon was restarted. With this update, jobs are executed only when the machine is rebooted.

BZ#480930

The crontab utility is now compiled as a position-independent executable (PIE), which enhances the security of the system.

BZ#529632

When the parent crond daemon was stopped, but a child crond daemon was running (executing a program), the "service crond status" command incorrectly reported that crond was running. The source code has been modified, and the "service crond status" command now correctly reports that crond is stopped.

BZ#541189

According to the pam(8) manual page, the cron daemon, crond, supports access control with PAM (Pluggable Authentication Module). However, the PAM configuration file for crond did not export environment variables correctly and, consequently, setting PAM variables via cron did not work. This update includes a corrected /etc/pam.d/crond file that exports environment variables correctly. Setting pam variables via cron now works as documented in the pam(8) manual page.

BZ#625016

Previously, the mcstransd daemon modified labels for the crond daemon. When the crond daemon attempted to use the modified label and mcstransd was not running, crond used an incorrect label. Consequently, Security-Enhanced Linux (SELinux) denials filled up the cron log, no jobs were executed, and crond had to be restarted. With this update, both mcstransd and crond use raw SELinux labels, which prevents the problem.

BZ#699620, BZ#699621

Previously, the crontab(1) and cron(8) manual pages contained multiple typographical errors. This update fixes those errors.

Enhancement

BZ#249512

Previously, the crontab utility did not use the Pluggable Authentication Module (PAM) for verification of users. As a consequence, a user could access crontab even if access had been restricted (usually by being denied in the access.conf file). With this update, crontab returns an error message that the user is not allowed to access crontab because of PAM configuration.

All vixie-cron users should upgrade to this updated package, which resolves these issues and adds this enhancement.

4.208. vsftpd

4.208.1. RHBA-2012:0187 — vsftpd bug fix and enhancement update

An updated vsftpd package that fixes three bugs and adds three enhancements is now available for Red Hat Enterprise Linux 5.

The vsftpd package includes a Very Secure FTP (File Transfer Protocol) daemon.

Bug Fixes

BZ#513828

The "delay_failed_login" and "max_login_fails" options, which can be set in the vsftpd.conf file, did not work correctly. Consequently, the user had an unlimited number of login attempts if the "userlist_enabled=YES" and "userlist_deny=NO" rules were specified in the vsftpd.conf file. The vsftpd daemon now properly uses a delay between two unsuccessful login attempts and also refuses any connection after a specified number of unsuccessful login attempts.

BZ#717409

The vsftpd daemon did not handle file transfer failures correctly if the ftp-data port was blocked on the FTP client. As a consequence, vsftpd became unresponsive under these circumstances. The updated vsftpd daemon now reports such failures to the FTP client and the data transfer is terminated as expected.

BZ#759364

An attempt to list files could lead to a data type overflow error if a directory contained files with owner's UID or GID that was higher then the maximum value of the "signed int" data type (that

is 2147483647). Subsequently, the FTP connection was terminated. With this update, vsftpd has been modified to support UIDs and GIDs up to the maximum value of the "unsigned int" data type (that is 4294967294). Directory content is now listed as expected in the scenario described.

Enhancements

BZ#638873

The vsftpd server previously did not support the UTF-8 feature. This update implements the UTF-8 feature for the vsftpd server in accordance with the Internationalization of the File Transfer Protocol (RFC 2640) standard.

BZ#641239

The "ls" command previously did not support square brackets as wildcard characters in FTP connections. This update improves wildcard characters support in vsftpd and square brackets can now be used in regular expressions with the "ls" command accordingly.

BZ#644083

With this update, vsftpd introduces the new "ssl_request_cert" option, which enables vsftpd to request certificates on incoming SSL connections.

All users of vsftpd are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.209. xen

4.209.1. RHSA-2011:1401 — Moderate: xen security and bug fix update

Updated xen packages that fix one security issue and three bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The xen packages contain administration tools and the xend service for managing the kernel-xen kernel for virtualization on Red Hat Enterprise Linux.

Security Fix

CVE-2011-3346

A buffer overflow flaw was found in the Xen hypervisor SCSI subsystem emulation. An unprivileged, local guest user could provide a large number of bytes that are used to zero out a fixed-sized buffer via a SAI READ CAPACITY SCSI command, overwriting memory and causing the guest to crash.

Bug Fixes

BZ#738608

Prior to this update, the vif-bridge script used a maximum transmission unit (MTU) of 1500 for a new Virtual Interface (VIF). As a result, the MTU of the VIF could differ from that of the target bridge. This update fixes the VIF hot-plug script so that the default MTU for new VIFs will match that of the target Xen hypervisor bridge. In combination with a new enough kernel (RHSA-2011:1386), this enables the use of jumbo frames in Xen hypervisor guests.

BZ#738610

Prior to this update, the network-bridge script set the MTU of the bridge to 1500. As a result, the MTU of the Xen hypervisor bridge could differ from that of the physical interface. This update fixes the network script so the MTU of the bridge can be set higher than 1500, thus also providing support for jumbo frames. Now, the MTU of the Xen hypervisor bridge will match that of the physical interface.

BZ#743850

Red Hat Enterprise Linux 5.6 introduced an optimized migration handling that speeds up the migration of guests with large memory. However, the new migration procedure can theoretically cause data corruption. While no cases were observed in practice, with this update, the xend daemon properly waits for correct device release before the guest is started on a destination machine, thus fixing this bug.

Note

Before a guest is using a new enough kernel (RHSA-2011:1386), the MTU of the VIF will drop back to 1500 (if it was set higher) after migration.

All xen users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the xend service must be restarted for this update to take effect.

4.209.2. RHBA-2012:0160 — xen bug fix and enhancement update

Updated *xen* packages that fix several bugs and add several enhancements are now available for Red Hat Enterprise Linux 5.

The *xen* packages contain administration tools and the **xend** service for managing the **kernel-xen** kernel for virtualization on Red Hat Enterprise Linux.

Bug Fixes

BZ#497080

When an attempt to suspend a virtual guest on a disk without enough free space had been made, the suspend operation failed. As Red Hat Enterprise Linux 5 does not support suspend cancellation, this action sometimes caused unexpected termination. With this update, an additional check for enough free space has been added to the code. Now, the suspend operation is cancelled before it starts in the described scenario.

BZ#661211

Due to limitations in the Red Hat Enterprise Linux 5 Xen hypervisor, Red Hat Enterprise Linux 6 guests running fully-virtualized under Red Hat Enterprise Linux 5 occasionally experience time

drift or fails to boot. This issue can be resolved by adding the **clocksource=acpi_pm** or **clocksource=jiffies** parameters to the kernel command line for the guest. Alternatively, if running under Red Hat Enterprise Linux 5.7 or newer, adding **hpet=0** to the guest configuration file also fixes this bug. However, these workarounds had serious impact on performance. A patch has been provided to address this issue and now, performance is mostly unaffected in the described scenario when one of the workarounds described above is used.

BZ#699615

Previously, checking status of xendomains, after starting them without anything to do, led to a failed status and no message was returned. With this update, checking xendomains properly reports the **stopped** state in the described scenario, thus fixing this bug.

BZ#703693

Due to incorrect rounding in the code, setting the ***maxmem*** parameter on HVM (hardware-assisted virtualization) guests equal to the size of actual memory failed. With this update, a proper rounding method has been provided and attempts to set ***maxmem*** as described now succeed.

BZ#706859

When the user connected to a guest's console more than once at the same time, the output on all connections was broken. With this update, only one connection is allowed to the console, thus preventing this bug.

BZ#713074

When a guest was started via the **libvirt** API without a serial port specified, the **-serial none** option was passed to the **qemu** command line. However, **Xen Qemu** did not support this option, resulting in an unexpected termination of the guest. With this update, support for the **none** option has been added to **Xen Qemu**.

BZ#714855

When resizing memory on a paravirtualized guest, information provided by the **xm list -l** command included incorrect memory size as it used an incorrect size variable. With this update, memory of the guest is read directly and correct memory size is reported in the described scenario.

BZ#717525

Xen Qemu uses an older protocol and previously, orphan **qemu-dm** processes were sometimes left in the memory when a guest was destroyed immediately after start. With this update, the protocol output is checked in the described scenario and **qemu-dm** instances are properly destroyed after a guest is destroyed, thus fixing this bug.

BZ#719294

Previously, obsolete routing tables were used on the network during a live migration of a HVM guest. Consequently, a guest using a network interface sometimes experienced a short network outage after the migration. With this update, fake packets are sent after a migration is complete to ensure the routing tables are correctly updated, thus fixing this bug.

BZ#733417

To set a large MTU (Maximum Transmission Unit) on a bridge needs to be done in a precise order of script executions. Previously, when trying to set a MTU on a bridge with no interfaces, the MTU was not accepted. With this update, the Xen network scripts have been reorganized in the code and large MTUs are now created correctly in the described scenario.

BZ#733667

An update to Xen in Red Hat Enterprise Linux 5.7 added functionality to unpause a migrating guest before the source copy of the guest was destroyed. However, this could cause problems when removing devices that could be used on both sides of the connection and, in case of block devices, could also corrupt the data. With this update, devices are released before the destination copy of a guest is unpaused, thus fixing this bug.

BZ#735993

When a disk configured as **sda:cdrom** was added to an HVM domain, wrong media type was set for such disk. This could change the disk order and result in an unbootable domain. With this update, the ***hd_index*** parameter is adjusted once and for all disks, thus preventing this bug.

BZ#737851

An update to Xen in Red Hat Enterprise Linux 5.7 optimized guest creation procedure to speed up block device creation. However, this procedure caused that CD-ROM devices failed to disconnect from a guest. This update re-enables the functionality to properly disconnect CD-ROM devices.

Enhancements

BZ#524624

Variable amount of memory overhead is needed for creating a guest. Previously, a guest virtual domain could not be created due to insufficient available memory. This update introduces a new configuration option that sets additional memory to be reserved for guest creation, thus fixing this bug.

BZ#697310

Previously, when a bridge was being created for Xen networking, a wrong MTU was set for the bridge and the MTU was subsequently discarded. As a result, guests could not use jumbo frames when the host was using them. This update applies MTU size from the bridge interface to both the **netback** and **tap** interfaces, enabling jumbo frames on guests.

BZ#746602

This update adds support for the GPT (GUID Partition Table) partition table, which was introduced in Fedora 16 paravirtualized guests as a replacement for MBR (Master Boot Record).

BZ#705831

Prior to this update, the **debug-keys** command was only accessible from the serial console. This update adds the **debug-keys** command to the **xm** utility.

All *xen* users are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.210. xenpv-win

4.210.1. RHBA-2012:0195 — xenpv-win bug fix update

An updated xenpv-win package that fixes various bugs is now available for Red Hat Enterprise Linux 5.

The xenpv-win package contains installation images for para-virtualized drivers for guests running Windows XP or later on Red Hat Enterprise Linux hosts. Para-virtualized drivers provide significant network and disk I/O performance improvements for fully virtualized guests over the same guests running with fully virtualized drivers.

This updated package provides CD-ROM images containing the para-virtualized network and disk drivers for instances of Windows XP or later, running on a Red Hat Enterprise Linux host.

Bug Fixes

BZ#718329

Due to different requirements imposed by Linux and Windows on the implementation of checksum offloading, Windows Server 2003 guests running with para-virtualized drivers previously experienced many TCP retransmissions and showed poor network performance. With this update, checksum offloading has been disabled in the drivers and TCP sessions on Windows Server 2003 guests no longer exhibit problematic behavior.

BZ#697999

Previously, the para-virtualized Xen network driver did not report when it consumed packets. As a result, when using traffic control on virtual networks, Windows virtual machines dropped packets. Now, the driver correctly implements the "rx-notify" feature, packet consumption is reported promptly to the network back end running on domain 0, and traffic control does not cause unexpected packet drops.

BZ#692961

Para-virtualized Xen drives did not handle properly the "MODE SENSE" command. Consequently, Windows guests failed to initialize a mirror or a striped dynamic volume that included a para-virtualized Xen drive, leaving the volume in a failed state. With this update, the "MODE SENSE" command implementation has been fixed and dynamic volumes now work properly with para-virtualized Xen drives.

BZ#685049

A variable was not reset to NULL when Windows XP sent a ScsiStopAdapter control message to the RHELSCSI driver. Consequently, when running the debug version of the drivers on Windows XP, an assertion failure was reported during hibernation. Now, the stored device extension is reset to NULL when the adapter is stopped and the assertion failure no longer occurs.

BZ#725342

Previously, Windows guests did not acknowledge the "xm shutdown -H" command run from a

host. Consequently, attempting to turn off a Windows virtual machine with "xm shutdown -H" failed. Furthermore, it prevented "xm shutdown" from working until the virtual machine was rebooted. Now, the para-virtualized Xen network driver triggers a shutdown of a virtual machine when "xm shutdown -H" is sent, thus fixing this bug.

BZ#657540

Due to different requirements imposed by Linux and Windows on the implementation of checksum offloading, Windows guests running with para-virtualized drivers were unable to communicate with other guests running on the same host. With this update, checksum offloading has been disabled in the drivers and communication between Windows guests running on the same host now works correctly.

BZ#734813

Para-virtualized Xen drives did not handle properly the "READ CAPACITY(16)" command. Consequently, the "SCSI compliance test" in the Windows Logo Kit failed. Now, the "READ CAPACITY(16)" command implementation has been fixed and the compliance tests for it no longer fail.

Note that this bug does not cause any known problem in normal operation.

All users of xenpv-win are advised to upgrade to this updated package, which fixes these bugs.

4.211. xinetd

4.211.1. RHBA-2012:0217 — xinetd bug fix and enhancement update

An updated xinetd package that fixes one bug and adds one enhancement is now available for Red Hat Enterprise Linux 5.

The xinet daemon (xinetd) is a secure replacement for inetd, the Internet services daemon. It provides access control for all services based on the address of the remote host and on time of access, and can prevent denial of service attacks.

Bug Fix

BZ#754444

Prior to this update, xinetd contuously logged the message "descriptors still set" when reconfiguring a client service while the client was running. This update modifies the underlying code so that services can be configured as expected.

Enhancement

BZ#639447

Prior to this update, xinetd did not respect the no_files limit defined in the limits configuration. This update allows to set a limit on the maximum number of files for a child service and adds the rlimit_files option to the xinetd configuration. Now, xinetd respects the no_files limit.

All users of xinetd are advised to upgrade to this updated package, which fixes this bug and adds this enhancement.

4.212. xkeyboard-config

4.212.1. RHEA-2011:1153 — xkeyboard-config enhancement update

An updated xkeyboard-config package that adds an enhancement is now available for Red Hat Enterprise Linux 5.

The xkeyboard-config package contains configuration data used by the X Keyboard Extension (XKB), which allows selection of keyboard layouts when using a graphical interface.

Enhancement

BZ#727839

The new Unicode character U+20B9 (the Rupee symbol) has been added to Indic keyboard layouts.

Users of xkeyboard-config are advised to upgrade to this updated package, which adds this enhancement.

4.212.2. RHEA-2012:0173 — xkeyboard-config enhancement update

An updated xkeyboard-config package that adds an enhancement is now available for Red Hat Enterprise Linux 5.

The xkeyboard-config package contains configuration data used by the X Keyboard Extension (XKB), which allows selection of keyboard layouts when using a graphical interface.

Enhancement

BZ#674491

The new Unicode character U+20B9 (the Rupee symbol) has been added to Indic keyboard layouts.

Users of xkeyboard-config are advised to upgrade to this updated package, which adds this enhancement.

4.213. xmlrpc-c

4.213.1. RHEA-2011:1237 — xmlrpc-c enhancement update

Updated xmrlpc-c packages that add an enhancement are now available for Red Hat Enterprise Linux 5.

XML-RPC is a way to make remote procedure calls over the Internet. It converts procedure calls into XML documents, sends them to a remote server using the HTTP protocol, and gets back the response as XML. The xmlrpc-c package provides a modular implementation of XML-RPC for the C programming language.

Enhancement

BZ#729795

As a solution to a security issue, GSSAPI (Generic Security Services Application Program Interface) credential delegation was disabled in the libcurl library. As a consequence,

applications using the xmlrpc-c package and relying on the delegation exhibited various issues and did not work properly. With this update, the GSSAPI_DELEGATION option has been introduced into xmlrpc-c in order to enable the credential delegation explicitly when applications need it.

Users of xmlrpc-c are advised to upgrade to these updated packages, which add this enhancement.

4.213.2. RHBA-2012:0179 — xmlrpc-c bug fix update

Updated xmlrpc-c packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

The xmlrpc-c utility provides a way to make remote procedure calls over the Internet. It converts the procedure call into an XML document, sends it to a remote server using HTTP, and gets back the response as XML.

Bug Fixes

BZ#727884, BZ#756704

Prior to this update, the Generic Security Services Application Program Interface (GSSAPI) credential delegation was disabled. As a consequence, applications using the xmlrpc-c package and relying on the delegation exhibited various issues and did not work as expected. This update adds the analogous GSSAPI_DELEGATION to xmlrpc-c to allow for credential delegation when applications need it.

All users of xmlrpc-c are advised to upgrade to these updated packages, which fix these bugs.

4.214. xorg-x11-drv-i810

4.214.1. RHBA-2012:0289 — xorg-x11-drv-i810 bug fix update

An updated xorg-x11-drv-i810 package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The xorg-x11-drv-i810 package contains an Intel integrated graphics video driver for the X.Org implementation of the X Window System.

Bug Fix

BZ#581897

Previously, various bugs in the LVDS (Low-voltage differential signaling) panel setup prevented the Intel graphics driver from being fully functional on Intel Core i3, i5 and i7 processors. Users could, for example, experience problems with dual head setups or problems caused by incorrect PLL (Phase Locked Loop) parameters, search algorithm or pipe depth. This update fixes all LVDS-related bugs, and so ensures correct behavior of the driver.

All users of xorg-x11-drv-i810 are advised to upgrade to this updated package, which fixes this bug.

4.215. xorg-x11-drv-mga

An updated xorg-x11-drv-mga package that fixes two bugs and adds one enhancement is now available for Red Hat Enterprise Linux 5.

The xorg-x11-drv-mga provides the Matrox video driver for the X Window System.

Bug Fixes

BZ#735713

Previously, the X Window System selected an incorrect monitor resolution if Extended Display Identification Data (EDID) could not be read (for example, when the monitor was unplugged on boot). As a consequence, the graphical screen was distorted. This was caused by a faulty mode selection heuristic for Matrox G200e chips. This update fixes the problem and the correct monitor resolution is now selected even if EDID is not available.

BZ#745089

Due to a bug in the mga driver, a shift could occur in the video screen on future Dell systems with Matrox G200eR2 chips. The screen output was corrupted, and windows and text were pushed around randomly. This update optimizes priority request control, and the screen is no longer corrupted on the aforementioned systems.

Enhancement

BZ#475269

This update adds support for screen resolution of 1920x1200 on ServerEngines Pilot 3 (Kronos 3) chips.

All users of xorg-x11-drv-mga are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.216. xorg-x11-drv-sis

4.216.1. RHBA-2011:1420 — xorg-x11-drv-sis bug fix update

An updated xorg-x11-drv-sis package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The xorg-x11-drv-sis package provides a video driver for SiS and XGI graphics chips for the X.Org implementation of the X Window System.

Bug Fix

BZ#730649

Due to a missing XGIPowerSaving() function call in the xgi video driver's source code, a server using XGI Z9-series graphics chipset was not able to recover from power-saving mode. With this update, the XGIPowerSaving() function call has been added and the server now recovers properly.

All users of xorg-x11-drv-sis are advised to upgrade to this updated package, which fixes this bug.

4.217. xorg-x11-server

4.217.1. RHSA-2011:1359 — Moderate: xorg-x11-server security update

Updated xorg-x11-server packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

X.Org is an open source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon.

Security Fixes

CVE-2010-4818

Multiple input sanitization flaws were found in the X.Org GLX (OpenGL extension to the X Window System) extension. A malicious, authorized client could use these flaws to crash the X.Org server or, potentially, execute arbitrary code with root privileges.

CVE-2010-4819

An input sanitization flaw was found in the X.Org Render extension. A malicious, authorized client could use this flaw to leak arbitrary memory from the X.Org server process, or possibly crash the X.Org server.

Users of xorg-x11-server should upgrade to these updated packages, which contain backported patches to resolve these issues. All running X.Org server instances must be restarted for this update to take effect.

4.217.2. RHSA-2012:0303 — Low: xorg-x11-server security and bug fix update

Updated xorg-x11-server packages that fix one security issue and various bugs are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

X.Org is an open source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon.

Security Fix

CVE-2011-4028

A flaw was found in the way the X.Org server handled lock files. A local user with access to the system console could use this flaw to determine the existence of a file in a directory not accessible to the user, via a symbolic link attack.

Red Hat would like to thank the researcher with the nickname vladz for reporting this issue.

Bug Fixes

BZ#596899

In rare cases, if the front and back buffer of the miDbePositionWindow() function were not both allocated in video memory, or were both allocated in system memory, the X Window System sometimes terminated unexpectedly. A patch has been provided to address this issue and X no longer crashes in the described scenario.

BZ#676270

Previously, when the miSetShape() function called the miRegionDestroy() function with a NULL region, X terminated unexpectedly if the backing store was enabled. Now, X no longer crashes in the described scenario.

BZ#529717

On certain workstations running in 32-bit mode, the X11 mouse cursor occasionally became stuck near the left edge of the X11 screen. A patch has been provided to address this issue and the mouse cursor no longer becomes stuck in the described scenario.

BZ#559964

On certain workstations with a dual-head graphics adapter using the r500 driver in Zaphod mode, the mouse pointer was confined to one monitor screen and could not move to the other screen. A patch has been provided to address this issue and the mouse cursor works properly across both screens.

BZ#674741

Due to a double free operation, Xvfb (X virtual framebuffer) terminated unexpectedly with a segmentation fault randomly when the last client disconnected, that is when the server reset. This bug has been fixed in the miDCCloseScreen() function and Xvfb no longer crashes.

BZ#454409

Starting the Xephyr server on an AMD64 or Intel 64 architecture with an integrated graphics adapter caused the server to terminate unexpectedly. This bug has been fixed in the code and Xephyr no longer crashes in the described scenario.

BZ#555000

Previously, when a client made a request bigger than 1/4th of the limit advertised in the BigRequestsEnable reply, the X server closed the connection unexpectedly. With this update, the maxBigRequestSize variable has been added to the code to check the size of client requests, thus fixing this bug.

BZ#588346

When an X client running on a big-endian system called the XineramaQueryScreens() function, the X server terminated unexpectedly. This bug has been fixed in the xf86Xinerama module and the X server no longer crashes in the described scenario.

BZ#740497

When installing Red Hat Enterprise Linux 5 on an IBM eServer System p blade server, the installer did not set the correct mode on the built-in KVM (Keyboard-Video-Mouse). Consequently, the graphical installer took a very long time to appear and then was displayed incorrectly. A patch has been provided to address this issue and the graphical installer now

works as expected in the described scenario. Note that this fix requires the Red Hat Enterprise Linux 5.8 kernel update.

BZ#649810

Lines longer than 46,340 pixels can be drawn with one of the coordinates being negative. However, for dashed lines, the miPolyBuildPoly() function overflowed the "int" type when setting up edges for a section of a dashed line. Consequently, dashed segments were not drawn at all. An upstream patch has been applied to address this issue and dashed lines are now drawn correctly.

All users of xorg-x11-server are advised to upgrade to these updated packages, which correct these issues. All running X.Org server instances must be restarted for this update to take effect.

4.218. xulrunner

4.218.1. RHSA-2012:0143 — Critical: xulrunner security update

Updated xulrunner packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

XULRunner provides the XUL Runtime environment for applications using the Gecko layout engine.

Security Fix

CVE-2011-3026

A heap-based buffer overflow flaw was found in the way XULRunner handled PNG (Portable Network Graphics) images. A web page containing a malicious PNG image could cause an application linked against XULRunner (such as Firefox) to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

All XULRunner users should upgrade to these updated packages, which correct this issue. After installing the update, applications using XULRunner must be restarted for the changes to take effect.

4.219. yaboot

4.219.1. RHBA-2012:0300 — yaboot bug fix update

An updated yaboot package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The yaboot package provides a boot loader for Open Firmware based PowerPC systems. It can be used to boot IBM eServer System p machines.

Bug Fix

BZ#755959

Prior to this update, the yaboot boot loader failed when either a ext4 or an encrypted partition

was defined on the primary disk drive. This update modifies the yaboot binary so that it accepts ext4 and encrypted partitions on the primary disk drive.

All users of yaboot are advised to upgrade to this updated package, which fixes this bug.

4.220. yp-tools

4.220.1. RHEA-2012:0204 — yp-tools enhancement update

An updated yp-tools package that adds one enhancement is now available for Red Hat Enterprise Linux 5.

The Network Information Service (NIS), formerly known as Sun Yellow Pages (YP), is a system that provides network information (login names, passwords, home directories, group information) to all machines on a network. NIS can enable users to log in on any machine on the network as long as the machine has the NIS client programs running and the user's password is recorded in the NIS passwd database.

Enhancement

BZ#682037

When using the /etc/passwd.adjunct configuration file, the previous version of the ypasswd client program did not recognize the salt used for hashing a new password and chose the Data Encryption Standard (DES) as the default hash function. This update introduces a new "YP_PASSWD_HASH" environment variable, which allows users to explicitly specify either "md5" (for the MD5 Message-Digest Algorithm) or "des" (DES) as the hash algorithm.

All users of yp-tools are advised to upgrade to this updated package, which adds this enhancement.

4.221. ypserv

4.221.1. RHBA-2012:0205 — ypserv bug fix and enhancement update

An updated ypserv package that fixes various bugs and adds one enhancement is now available for Red Hat Enterprise Linux 5.

The ypserv utility provides network information (login names, passwords, home directories, group information) to all of the machines on a network. It can enable users to log in on any machine on the network as long as the machine has the Network Information Service (NIS) client programs running and the user's password is recorded in the NIS passwd database. NIS was formerly known as Sun Yellow Pages (YP).

Bug Fixes

BZ#747317

Previously, the rpc.yppasswdd daemon reported success even if the daemon was not able to write into a shadow file (for example, because of the incorrect SELinux context). With this update, an error is logged in syslog, and rpc.yppasswdd now reports failure in the described scenario.

BZ#403621

Due to the invalid ypdb_close() call, ypserv's virtual memory could in rare cases grow to a large size. As a consequence, ypserv failed to respond to Network Information Service (NIS) queries and had to be restarted. This update removes the invalid ypdb_close() call so that the amount of memory used remains at a reasonable size.

BZ#481780

Previously, when the user updated the ypserv package, the file /var/yp/Makefile was replaced, and any changes that the user had made in this file were overwritten. The file is now regarded as a config file, and is no longer replaced so that user's changes are preserved.

BZ#681699

Due to a string concatenation error in the code, running the "yppasswdd" command with the "-x" option in order to pass data to an external program to update the source files and maps, could have caused garbage characters to be inserted in front of the username. This caused the output to become unparseable. With this update, the operation is changed to a string-copy, so that the username is no longer corrupted when using the "-x" option.

BZ#695754

Previously, error messages of the rpc.yppasswdd utility were unclear when running the "yppasswdd" command with the "-x" option in order to pass data to an external program. This update adds quotation marks to error messages so that they can be easily read.

BZ#699662

Previously, there was no reference to the YPSERV_ARGS and YPXFRD variables in the sysconfig.txt file, neither in the ypserv manual pages. This update adds the YPSERV_ARGS and YPXFRD usage information to the ypserv manual pages.

BZ#707195

Prior to this update, the ypserv package did not contain a file describing what license the software used. This update adds the COPYING file which contains the license information.

BZ#712239

Previously, the yppush(8) manual page did not describe how to force the yppush utility to use a static port. The yppush(8) manual page has been modified to mention that the static port number can be set in /var/yp/Makefile.

BZ#743587

Prior to this update, the root user could see old passwords of other users. This was caused by a change request being logged using syslog when running the "yppaswdd" command with the "-x" option to pass data to an external program. With this update, the old password hash and the new password hash are cleared in syslog and the root user can no longer view the old passwords of other users.

Enhancements

BZ#679848

Prior to this update, users were not able to change their passwords by running the "yppasswd"

command if using the passwd.adjunct file, which prevents disclosing the encrypted passwords. With this update, users are now able to change their passwords.

All users of ypserv are advised to upgrade to this updated package, which fixes these bugs and provides this enhancement.

4.222. yum

4.222.1. RHBA-2012:0273 — yum bug fix and enhancement update

An updated yum package that fixes one bug and adds one enhancement is now available for Red Hat Enterprise Linux 5.

Yum is a utility that can check for updates and automatically download and install updated RPM packages. Dependencies are obtained and downloaded automatically, prompting the user for permission as necessary.

Bug Fix

BZ#552279

Prior to this update, the nice level for daemon restarts was inherited from the environment. As a consequence, daemons updated by yum-updatesd restarted at a lower priority and changed the system behaviour. This update modifies the underlying code so that the daemons are now at normal priority of 0.

Enhancement

BZ#662175

This update adds the commands update-to and upgrade-to to the yum package, which allow to upgrade a certain package to a specific version.

All users of yum are advised to upgrade to this updated package, which fixes this bug and adds this enhancement.

4.223. yum-rhn-plugin

4.223.1. RHBA-2011:1281 — yum-rhn-plugin bug fix update

An updated yum-rhn-plugin package that fixes three bugs is now available for Red Hat Enterprise Linux 5.

The yum-rhn-plugin package provides a plug-in that allows Yum to access a Red Hat Network server for software updates.

Bug Fixes

BZ#736058

When a user attempted to run the rhn_check utility with no additional command line options, the package installation failed with no error reported to the user and the following error message was logged on the server:

Error while executing packages action: empty transaction [[6]]

This update adapts the underlying source code to ensure the command line options are handled correctly, and the rhn_check utility now works as expected.

BZ#736060

Previously, running the pirut package manager with no command line options rendered it unable to access repositories provided by Red Hat Network or Red Hat Network Satellite. This was caused by an error in the yum-rhn-plugin package. With this update, this error has been fixed, and pirut no longer fails to access these repositories.

BZ#736250

Due to an error in the option parsing algorithm, the Package Manager incorrectly prompted the user to register the system with Red Hat Network every time it was started. With this update, the relevant part of the source code has been corrected, and the Package Manager no longer prompts users to register already registered systems.

All users of yum-rhn-plugin are advised to upgrade to this updated package, which fixes these bugs.

4.223.2. RHBA-2011:1198 — yum-rhn-plugin bug fix update

An updated yum-rhn-plugin package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The yum-rhn-plugin package provides rhnplugin, a plug-in that allows Yum to access a Red Hat Network server for software updates.

Bug Fix

BZ#732427

Prior to this update, rhnplugin always downloaded all available repository metadata, including the filelist.xml and others.xml files, which are not required for regular Yum transactions. To prevent unnecessary disk space consumption, this update adapts rhnplugin to download only the metadata required for a particular Yum transaction.

All users of yum-rhn-plugin are advised to upgrade to this updated package, which fixes this bug.

4.223.3. RHBA-2012:0162 — yum-rhn-plugin bug fix update

An updated *yum-rhn-plugin* package that fixes multiple bugs is now available for Red Hat Enterprise Linux 5.

The *yum-rhn-plugin* package provides support for connecting to Red Hat Network (RHN). Systems registered with RHN are able to update and install packages from Red Hat Network.

Bug Fixes

BZ#709241

Previously, the repository cache in the **`/var/cache/yum/rhnplugin.repos`** file was not cleaned up properly after a Red Hat Network channel was removed from the list of configured repositories. Consequently, the first run of the **`yum repolist`** failed with an error. This update fixes the cache cleaning procedure and the problem no longer occurs.

BZ#711829

Previously *yum-rhn-plugin* did not disable Location-Aware Updates when the **useNoSSLForPackages** option was set. This update adds the **useNoSSLForPackages** option to the **/etc/sysconfig/rhn/up2date** configuration file and corrects the option's behavior so that when enabled (that is, when set to **1**), the **HTTP** protocol is used for downloading repository metadata and RPM packages. Enabling this option correctly disables Location-Aware Updates; the option can be used only over **HTTPS**.

BZ#726017

Previously, the **--nogpgcheck** option of the **yum install** command failed to override the **gpgcheck=1** configuration option in the **/etc/yum/plugins.d/rhnplugin.conf** file. Consequently, *yum-rhn-plugin* ignored the **--nogpgcheck** option. When installing a package with no signature, the process finished with a message that the package was not signed and returned error code **1**. With this update, the underlying code has been modified and the package installation finishes successfully in this scenario.

BZ#726644

Previously, if a Python application ran a **yum** command that loaded *yum-rhn-plugin*, the sys.path value, which contains Python module paths, was modified. If the application submodules had the same name as yum submodules, the applications failed to load the correct modules and could be rendered unusable. With this update, **yum-rhn-plugin** no longer changes the sys.path and the problem no longer occurs.

BZ#729584

If *yum-rhn-plugin* was installed, various yum utilities (such as yum help and repository filtering) did not work correctly. This happened due to incorrect parsing of command arguments. This update fixes the parsing of plug-in arguments and the utilities work as expected.

BZ#729657

Previously, the **rhn_client** client populated the package list with all packages after Red Hat Network setup. Consequently, the **rhnplugin** tool downloaded metadata of all repositories, including the **others.xml** and **filelist.xml** files, which are generally not required for regular yum usage. With this update, **rhn_check** no longer populates the list of packages after initial setup and rhnplugin downloads only relevant metadata.

BZ#729949

Previously, the **yum repolist -C** command, which lists the configured repositories without accessing network only using the system cache, failed with the following error message:

```
TypeError: iteration over non-sequence
```

With this update, the underlying code has been modified and the command works as expected.

BZ#734492

Due to an error in the option parsing algorithm, the Package Manager incorrectly prompted the user to register the system with Red Hat Network every time it was started. With this update, the relevant part of the source code has been corrected and the Package Manager no longer

prompts users to register already registered systems.

BZ#734965

Previously, running the **pirut** package manager with no command line options rendered it unable to access repositories provided by Red Hat Network or Red Hat Network Satellite. This was caused by an error in the *yum-rhn-plugin* package. With this update, this error has been fixed and pirut no longer fails to access these repositories.

BZ#735282

When the user attempted to run the **rhn_client** utility with no additional command-line options, the package installation failed with no error reported to the user and the following error message was logged on the server:

```
Error while executing packages action: empty transaction [[6]]
```

This update adapts the underlying source code to ensure the command-line options are handled correctly and the rhn_check utility now works as expected.

BZ#738193

If the **rhnplugin.repos** file contained outdated information, for example, an RHN channel was previously removed from the server, the **rhn_check** utility failed with the following error when it attempted to retrieve metadata of an unavailable channel:

```
yum.Errors.RepoError: Cannot retrieve repository metadata (repomd.xml) for
repository: rhel-i386-server-5. Please verify its path and try again
```

With this update, metadata is no longer retrieved from unavailable channels and the problem no longer occurs.

Users of *yum-rhn-plugin* are advised to upgrade to this updated package, which fixes these bugs.

4.224. yum-utils

4.224.1. RHBA-2012:0281 — yum-utils bug fix and enhancement update

Updated yum-utils packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 5.

The yum-utils packages provide a collection of utilities and examples for the yum package manager to make yum easier and more powerful to use.

Bug Fixes

BZ#543649

Previously, a yum transaction could fail with the message that a kmod package was already installed if a kmod plug-in was installed and the "installforallkernels" option set in the /etc/yum/pluginconf.d/kmod.conf file. This happened when the requested packages were located in a different repository due to an incorrect handling of repository ID resolution. With this update, the respective method has been corrected and such yum transactions are executed successfully as expected.

BZ#732596

The manual page of the reposync tool contained an imprecise description of the "--arch" option. This update enhances the "--arch" option documentation.

BZ#711768

Previously, a package download could fail with the error message that the package already existed and appeared to be complete. This happened if the latest version of the package was available in multiple repositories because the yumdownloader tool attempted to download the package from all the repositories. With this update, yum downloads such a package only from one repository and the update process finishes successfully in the described scenario.

BZ#703372

The repomanage command failed with a traceback if it was executed on an invalid repository path. With this update, the underlying code has been modified and the command returns the "Error accessing directory" error message under these circumstances.

BZ#631843

Previously, the "--count" option was incorrectly located in the "OLDKERNELS OPTIONS" section of manual pages. However, "--count" is a general option. With this update, the "--count" option has been moved to the "GENERAL OPTIONS" section.

BZ#496580

Previously, the "package-cleanup --oldkernels" command could not handle kernel-PAE and kernel-xen packages and the command terminated with the following error message:

Error all kernel rpms are set to be removed.

With this update, the kernel-PAE and kernel-xen packages are handled correctly and the specified number of packages (by default, two packages) is kept after the command has been issued.

Enhancement

BZ#530150

This update adds the manual page for the debuginfo-install command.

All users of yum-utils are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.225. zsh

4.225.1. RHBA-2012:0274 — zsh bug fix update

Updated zsh packages that fix three bugs are now available for Red Hat Enterprise Linux 5.

The zsh shell is a command interpreter which can be used as an interactive login shell and as a shell

script command processor. Zsh resembles the ksh shell (the Korn shell), but includes many enhancements. Zsh supports command line editing, built-in spelling correction, programmable command completion, shell functions (with autoloading), a history mechanism, and more.

Bug Fixes

BZ#700722

Prior to this update, the compdef utility prevented more than three commands from using one completion service. As a consequence, compdef failed with the error message "unknown command or service: mount". This update corrects the underlying source code so that now more than 3 commands can use one completion service.

BZ#706029

Prior to this update, zsh could, under certain circumstances, keep the Process ID (PID) of terminated or suspended processes in the jobs list. As a consequence, zsh waited infinitely for already terminated or suspended processes. This update no longer returns the terminated PID and zsh now runs as expected.

BZ#733582

Prior to this update, zsh could be interrupted when running the fork() option if the malloc arena was still locked. As a consequence, zsh could become indefinitely suspended when the malloc() function got called. With this update, signals are queued before the fork to avoid interruptions.

All users of the zsh shell are advised to upgrade to these updated packages, which fix these bugs.

Package Manifest

This appendix is a list of all package changes since the release of Red Hat Enterprise Linux 5.7.

A.1. Server

A.1.1. Added Packages

binutils220-2.20.51.0.2-5.29.el5

- Group: Development/Tools
- Summary: Binary utilities for the preview of GCC version 4.4
- Description: The binutils220 package contains the assembler and objdump utility for the preview of GCC version 4.4.

iotop-0.4.3-4.el5

- Group: Applications/System
- Summary: Top like utility for I/O
- Description: Linux has always been able to show how much I/O was going on (the bi and bo columns of the vmstat 1 command). iotop is a Python program with a top like UI used to show of behalf of which process is the I/O going on.

mysql-connector-odbc64-5.1.8-1.el5

- Group: System Environment/Libraries
- Summary: ODBC driver for MySQL
- Description: An ODBC (rev 3) driver for MySQL, for use with unixODBC64.

postgresql-odbc64-09.00.0200-1.el5

- Group: Applications/Databases
- Summary: PostgreSQL ODBC driver
- Description: This package includes the driver needed for applications to access a PostgreSQL system via ODBC (Open Database Connectivity). This version is for use with unixODBC64.

python-ctypes-1.0.2-3.el5

- Group: Development/Libraries
- Summary: Create and manipulate C data types from Python
- Description: python-ctypes is a python module to create and manipulate C data types in Python, and to call functions in dynamic link libraries/shared dlls. It allows wrapping these libraries in pure Python.

subscription-manager-migration-data-1.11-1.el5

- Group: System Environment/Base
- Summary: RHN Classic to RHSM migration data

- Description: This package provides certificates for migrating a system from RHN Classic to RHSM.

unixODBC64-2.2.14-3.el5

- Group: System Environment/Libraries
- Summary: A complete ODBC driver manager for Linux
- Description: Install unixODBC64 if you want to access databases through ODBC, and you need to use the corrected 64-bit ABI used in unixODBC 2.2.12 and up. This base package provides documentation and command-line utility programs, but is not required for client applications to make use of unixODBC64. You will also need the mysql-connector-odbc64 package if you want to access a MySQL database, and/or the postgresql-odbc64 package for PostgreSQL.

virt-who-0.5-5.el5

- Group: System Environment/Base
- Summary: Agent for reporting virtual guest IDs to subscription-manager
- Description: Agent that collects information about virtual guests present in the system and report them to the subscription manager.

A.1.2. Dropped Packages

None

A.1.3. Updated Packages

Cluster_Administration-5.2-1 - Cluster_Administration-5.8-1.el5

- Group: Documentation
- Summary: Red Hat Cluster for Red Hat Enterprise Linux
- Description: Configuring and Managing a Red Hat Cluster describes the configuration and management of Red Hat cluster systems for Red Hat Enterprise Linux 5.8 It does not include information about Red Hat Linux Virtual Servers (LVS). Information about installing and configuring LVS is in a separate document.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

Deployment_Guide-5.2-11 - Deployment_Guide-5.8-1.el5

- Group: Documentation
- Summary: Deployment Guide
- Description: This Deployment Guide documents relevant information regarding the

deployment, configuration and administration of Red Hat Enterprise Linux 5.8.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

Global_File_System-5.2-1 - Global_File_System-5.8-1.el5

- Group: Documentation
- Summary: Red Hat Global File System
- Description: This book provides information about installing, configuring, and maintaining Red Hat GFS (Red Hat Global File System) for Red Hat Enterprise Linux 5.8.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ImageMagick-6.2.8.0-4.el5_5.3 - ImageMagick-6.2.8.0-12.el5

- Group: Applications/Multimedia
- Summary: An X application for displaying and manipulating images.
- Description: ImageMagick(TM) is an image display and manipulation tool for the X Window System. ImageMagick can read and write JPEG, TIFF, PNM, GIF, and Photo CD image formats. It can resize, rotate, sharpen, color reduce, or add special effects to an image, and when finished you can either save the completed work in the original format or a different one. ImageMagick also includes command line programs for creating animated or transparent .gifs, creating composite images, creating thumbnail images, and more. ImageMagick is one of your choices if you need a program to manipulate and dis play images. If you want to develop your own applications which use ImageMagick code or APIs, you need to install ImageMagick-devel as well.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

MySQL-python-1.2.1-1 - MySQL-python-1.2.3-0.1.c1.el5

- Group: Development/Libraries
- Summary: An interface to MySQL
- Description: Python interface to MySQL MySQLdb is an interface to the popular MySQL database server for Python. The design goals are: - Compliance with Python database API version 2.0 - Thread-safety - Thread-friendliness (threads will not block each other) - Compatibility with MySQL 3.23 and up This module should be mostly compatible with an older interface written by Joe Skinner and others. However, the older version is a) not thread-friendly, b) written for MySQL 3.21, c) apparently not actively maintained. No code from that version is used in MySQLdb.
- Added Dependencies:
  - python-devel
  - python-setuptools
- Removed Dependencies:
  - Distutils
  - gcc
  - python
  - python-devel >= 2.4
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

OpenIPMI-2.0.16-11.el5 - OpenIPMI-2.0.16-12.el5

- Group: System Environment/Base
- Summary: OpenIPMI (Intelligent Platform Management Interface) library and tools
- Description: The Open IPMI project aims to develop an open code base to allow access to platform information using Intelligent Platform Management Interface (IPMI). This package contains the tools of the OpenIPMI project.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

PyXML-0.8.4-4.el5_4.2 - PyXML-0.8.4-6.el5

- Group: Development/Libraries
- Summary: XML libraries for python.

- Description: An XML package for Python. The distribution contains a validating XML parser, an implementation of the SAX and DOM programming interfaces and an interface to the Expat parser.
- Added Dependencies:
  - python-setuptools
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

SDL-1.2.10-8.el5 - SDL-1.2.10-9.el5

- Group: System Environment/Libraries
- Summary: A cross-platform multimedia library.
- Description: Simple DirectMedia Layer (SDL) is a cross-platform multimedia library designed to provide fast access to the graphics frame buffer and audio device.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

Virtualization-5.2-11 - Virtualization-5.8-1.el5

- Group: Documentation
- Summary: Virtualization Guide
- Description: The Red Hat Enterprise Linux Virtualization Guide contains information on installation, configuring, administering, tips, tricks and troubleshooting virtualization technologies used in Red Hat Enterprise Linux.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

acl-2.2.39-6.el5 - acl-2.2.39-8.el5

- Group: System Environment/Base
- Summary: Access control list utilities.
- Description: This package contains the getfacl and setfacl utilities needed for manipulating access control lists.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

acpid-1.0.4-9.el5_4.2 - acpid-1.0.4-12.el5

- Group: System Environment/Daemons
- Summary: ACPI Event Daemon
- Description: acpid is a daemon that dispatches ACPI events to user-space programs.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

alsa-utils-1.0.17-1.el5 - alsa-utils-1.0.17-6.el5

- Group: Applications/Multimedia
- Summary: Advanced Linux Sound Architecture (ALSA) utilities
- Description: This package contains command line utilities for the Advanced Linux Sound Architecture (ALSA).
- Added Dependencies:
  - autoconf
  - automake
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

amanda-2.5.0p2-8.el5 - amanda-2.5.0p2-9.el5

- Group: Applications/System
- Summary: A network-capable tape backup solution.
- Description: AMANDA, the Advanced Maryland Automatic Network Disk Archiver, is a backup system that allows the administrator of a LAN to set up a single master backup server to back up multiple hosts to one or more tape drives or disk files. AMANDA uses native dump and/or GNU tar facilities and can back up a large number of workstations running multiple versions of Unix. Newer versions of AMANDA (including this version) can use SAMBA to back up Microsoft(TM) Windows95/NT hosts. The amanda package contains the core AMANDA programs and will need to be installed on both AMANDA clients and AMANDA servers. Note that you will have to install the amanda-client and/or amanda-server packages as well.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

anaconda-11.1.2.242-1 - anaconda-11.1.2.250-1

- Group: Applications/System
- Summary: Graphical system installer
- Description: The anaconda package contains the program which was used to install your system. These files are of little use on an already installed system.
- Added Dependencies:
  - kudzu-devel >= 1.2.57.1.26-3
  - libdhcp-devel >= 1.20-13
- Removed Dependencies:
  - kudzu-devel >= 1.2.57.1.26-1
  - libdhcp-devel >= 1.20-10
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

arptables_jf-0.0.8-8 - arptables_jf-0.0.8-11.el5

- Group: System Environment/Base
- Summary: Userspace control program for the arptables network filter.
- Description: The arptables_jf utility controls the arpfilter network packet filtering code in the Linux kernel. You do not need this program for normal network firewalling. If you need to manually control which arp requests and/or replies this machine accepts and sends, you should install this package.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

aspell-0.60.3-7.1 - aspell-0.60.3-12

- Group: Applications/Text
- Summary: A spelling checker.
- Description: GNU Aspell is a spell checker designed to eventually replace Ispell. It can either be used as a library or as an independent spell checker. Its main feature is that it does a much better job of coming up with possible suggestions than just about any other spell checker out there for the English language, including Ispell and Microsoft Word. It also has many other technical enhancements over Ispell such as using shared memory for dictionaries and intelligently handling personal dictionaries when more than one Aspell process is open at once.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

aspell-sr-0.02-1.2.1 - aspell-sr-0.02-2

- Group: Applications/Text
- Summary: Serbian dictionaries for Aspell.
- Description: Provides the word list/dictionaries for the following: Serbian
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

audit-1.7.18-2.el5 - audit-1.8-2.el5

- Group: System Environment/Daemons

- Summary: User space tools for 2.6 kernel auditing
- Description: The audit package contains the user space utilities for storing and searching the audit records generate by the audit subsystem in the Linux 2.6 kernel.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

autofs-5.0.1-0.rc2.156.el5 - autofs-5.0.1-0.rc2.163.el5

- Group: System Environment/Daemons
- Summary: A tool for automatically mounting and unmounting filesystems.
- Description: autofs is a daemon which automatically mounts filesystems when you use them, and unmounts them later when you are not using them. This can include network filesystems, CD-ROMs, floppies, and so forth.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

bind-9.3.6-16.P1.el5 - bind-9.3.6-20.P1.el5

- Group: System Environment/Daemons
- Summary: The Berkeley Internet Name Domain (BIND) DNS (Domain Name System) server.
- Description: BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating properly.
- Added Dependencies:
  - docbook-style-xsl
  - libxslt
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

bind97-9.7.0-6.P2.el5_6.3 - bind97-9.7.0-6.P2.el5_7.4

- Group: System Environment/Daemons
- Summary: The Berkeley Internet Name Domain (BIND) DNS (Domain Name System) server
- Description: BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating properly.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

binutils-2.17.50.0.6-14.el5 - binutils-2.17.50.0.6-20.el5

- Group: Development/Tools
- Summary: A GNU collection of binary utilities.
- Description: Binutils is a collection of binary utilities, including ar (for creating, modifying and extracting from archives), as (a family of GNU assemblers), gprof (for displaying call graph profile data), ld (the GNU linker), nm (for listing symbols from object files), objcopy (for copying and translating object files), objdump (for displaying information from object files), ranlib (for generating an index for the contents of an archive), size (for listing the section sizes of an object or archive file), strings (for listing printable strings from files), strip (for discarding symbols), and addr2line (for converting addresses to file and line).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

boost-1.33.1-10.el5 - boost-1.33.1-15.el5

- Group: System Environment/Libraries
- Summary: The Boost C++ Libraries
- Description: Boost provides free peer-reviewed portable C++ source libraries. The emphasis is on libraries which work well with the C++ Standard Library, in the hopes of establishing "existing practice" for extensions and providing reference implementations so that the Boost libraries are suitable for eventual standardization. (Some of the libraries have already been proposed for inclusion in the C++ Standards Committee's upcoming C++ Standard Library Technical Report.)

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

bootparamd-0.17-26.el5 - bootparamd-0.17-26.el5_7.1

- Group: System Environment/Daemons
- Summary: A server process which provides boot information to diskless clients.
- Description: The bootparamd process provides bootparamd, a server process which provides the information needed by diskless clients in order for them to successfully boot. Bootparamd looks first in /etc/bootparams for an entry for that particular client; if a local bootparams file doesn't exist, it looks at the appropriate Network Information Service (NIS) map. Some network boot loaders (notably Sun's) rely on special boot server code on the server, in addition to the RARP and TFTP servers. This bootparamd server process is compatible with SunOS bootparam clients and servers which need that boot server code. You should install bootparamd if you need to provide boot information to diskless clients on your network.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

busybox-1.2.0-10.el5 - busybox-1.2.0-13.el5

- Group: System Environment/Shells
- Summary: Statically linked binary providing simplified versions of system commands
- Description: Busybox is a single binary which includes versions of a large number of system commands, including a shell. This package can be very useful for recovering from certain types of system failures, particularly those involving broken shared libraries.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cdparanoia-alpha9.8-27.2 - cdparanoia-alpha9.8-28

- Group: Applications/Multimedia
- Summary: A Compact Disc Digital Audio (CDDA) extraction tool (or ripper).
- Description: Cdparanoia (Paranoia III) reads digital audio directly from a CD, then writes the data to a file or pipe in WAV, AIFC or raw 16 bit linear PCM format. Cdparanoia doesn't contain any extra features (like the ones included in the cdda2wav sampling utility). Instead, cdparanoia's strength lies in its ability to handle a variety of hardware, including inexpensive drives prone to misalignment, frame jitter and loss of streaming during atomic reads. Cdparanoia is also good at reading and repairing data from damaged CDs.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

certmonger-0.42-1.el5 - certmonger-0.50-3.el5

- Group: System Environment/Daemons
- Summary: Certificate status monitor and PKI enrollment client
- Description: Certmonger is a service which is primarily concerned with getting your system enrolled with a certificate authority (CA) and keeping it enrolled.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

clustermon-0.12.1-2.el5 - clustermon-0.12.1-7.el5

- Group: System Environment/Base
- Summary: Monitoring and management of Red Hat Enterprise Linux Cluster Suite
- Description: This package contains Red Hat Enterprise Linux Cluster Suite SNMP/CIM module/agent/provider.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

cman-2.0.115-85.el5 - cman-2.0.115-96.el5

- Group: System Environment/Base
- Summary: cman - The Cluster Manager
- Description: cman - The Cluster Manager
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cmirror-1.1.39-10.el5 - cmirror-1.1.39-13.el5

- Group: System Environment/Base
- Summary: cmirror - The Cluster Mirror Package
- Description: cmirror - Cluster Mirroring
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

comps-extras-11.1-1.1 - comps-extras-11.4-1

- Group: Applications/System
- Summary: Images for components included in Fedora
- Description: This package contains images for the components included in Fedora.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

conga-0.12.2-32.el5 - conga-0.12.2-51.el5

- Group: System Environment/Base
- Summary: Remote Management System
- Description: Conga is a project developing management system for remote stations. It consists of luci, https frontend, and ricci, secure daemon that dispatches incoming messages to underlying management modules.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

crash-4.1.2-8.el5 - crash-5.1.8-1.el5

- Group: Development/Debuggers
- Summary: Kernel crash and live system analysis utility
- Description: The core analysis suite is a self-contained tool that can be used to investigate either live systems, kernel core dumps created from the netdump, diskdump and kdump packages from Red Hat Linux, the mcore kernel patch offered by Mission Critical Linux, or the LKCD kernel patch.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cups-1.3.7-26.el5_6.1 - cups-1.3.7-30.el5

- Group: System Environment/Daemons
- Summary: Common Unix Printing System
- Description: The Common UNIX Printing System provides a portable printing layer for UNIX® operating systems. It has been developed by Easy Software Products to promote a standard printing solution for all UNIX vendors and users. CUPS provides the System V and Berkeley command-line interfaces.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

curl-7.15.5-9.el5_6.3 - curl-7.15.5-15.el5

- Group: Applications/Internet
- Summary: A utility for getting files from remote servers (FTP, HTTP, and others).
- Description: cURL is a tool for getting files from FTP, HTTP, Gopher, Telnet, and Dict servers, using any of the supported protocols. cURL is designed to work without user interaction or any kind of interactivity. cURL offers many useful capabilities, like proxy support, user authentication, FTP upload, HTTP post, and file transfer resume.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cvs-1.11.22-7.el5 - cvs-1.11.22-11.el5

- Group: Development/Tools
- Summary: A version control system.
- Description: CVS (Concurrent Versions System) is a version control system that can record the history of your files (usually, but not always, source code). CVS only stores the differences between versions, instead of every version of every file you have ever created. CVS also keeps a log of who, when, and why changes occurred. CVS is very helpful for managing releases and controlling the concurrent editing of source files among multiple authors. Instead of providing version control for a collection of files in a single directory, CVS provides version control for a hierarchical collection of directories consisting of revision controlled files. These directories and files can then be combined together to form a software release.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cyrus-imapd-2.3.7-12.el5 - cyrus-imapd-2.3.7-12.el5_7.2

- Group: System Environment/Daemons
- Summary: A high-performance mail server with IMAP, POP3, NNTP and SIEVE support
- Description: The cyrus-imapd package contains the core of the Cyrus IMAP server. It is a

scaleable enterprise mail system designed for use from small to large enterprise environments using standards-based internet mail technologies. A full Cyrus IMAP implementation allows a seamless mail and bulletin board environment to be set up across multiple servers. It differs from other IMAP server implementations in that it is run on "sealed" servers, where users are not normally permitted to log in and have no system account on the server. The mailbox database is stored in parts of the filesystem that are private to the Cyrus IMAP server. All user access to mail is through software using the IMAP, POP3 or KPOP protocols. It also includes support for virtual domains, NNTP, mailbox annotations, and much more. The private mailbox database design gives the server large advantages in efficiency, scalability and administratability. Multiple concurrent read/write connections to the same mailbox are permitted. The server supports access control lists on mailboxes and storage quotas on mailbox hierarchies. The Cyrus IMAP server supports the IMAP4rev1 protocol described in RFC 3501. IMAP4rev1 has been approved as a proposed standard. It supports any authentication mechanism available from the SASL library, imaps/pop3s/nntps (IMAP/POP3/NNTP encrypted using SSL and TLSv1) can be used for security. The server supports single instance store where possible when an email message is addressed to multiple recipients, SIEVE provides server side email filtering.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dapl-2.0.25-2.el5_6.1 - dapl-2.0.25-2.3.el5

- Group: System Environment/Libraries
- Summary: Library providing access to the DAT 1.2 and 2.0 APIs
- Description: libdat and libdapl provide a userspace implementation of the DAT 1.2 and 2.0 API that is built to natively support InfiniBand/iWARP network technology.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dbus-1.1.2-15.el5_6 - dbus-1.1.2-16.el5_7

- Group: System Environment/Libraries
- Summary: D-BUS message bus
- Description: D-BUS is a system for sending messages between applications. It is used both for the systemwide message bus service, and as a per-user-login-session messaging facility.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

device-mapper-1.02.63-4.el5 - device-mapper-1.02.67-2.el5

- Group: System Environment/Base
- Summary: device mapper library
- Description: This package contains the supporting userspace files (libdevmapper and dmsetup) for the device-mapper.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

device-mapper-multipath-0.4.7-46.el5 - device-mapper-multipath-0.4.7-48.el5

- Group: System Environment/Base
- Summary: Tools to manage multipath devices using device-mapper.
- Description: device-mapper-multipath provides tools to manage multipath devices by instructing the device-mapper multipath kernel module what to do. The tools are : * multipath : Scan the system for multipath devices and assemble them. * multipathd : Detects when paths fail and execs multipath to update things.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dhcp-3.0.5-29.el5 - dhcp-3.0.5-31.el5

- Group: System Environment/Daemons
- Summary: DHCP (Dynamic Host Configuration Protocol) server and relay agent.
- Description: DHCP (Dynamic Host Configuration Protocol) is a protocol which allows

individual devices on an IP network to get their own network configuration information (IP address, subnetmask, broadcast address, etc.) from a DHCP server. The overall purpose of DHCP is to make it easier to administer a large network. The dhcp package includes the ISC DHCP service and relay agent. To use DHCP on your network, install a DHCP service (or relay agent), and on clients run a DHCP client daemon. The dhcp package provides the ISC DHCP service and relay agent.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dovecot-1.0.7-7.el5 - dovecot-1.0.7-7.el5_7.1

- Group: System Environment/Daemons
- Summary: Dovecot Secure imap server
- Description: Dovecot is an IMAP server for Linux/UNIX-like systems, written with security primarily in mind. It also contains a small POP3 server. It supports mail in either of maildir or mbox formats.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dstat-0.6.6-3.el5_4.1 - dstat-0.6.6-5.el5

- Group: System Environment/Base
- Summary: Versatile resource statistics tool
- Description: Dstat is a versatile replacement for vmstat, iostat, netstat and ifstat. Dstat overcomes some of their limitations and adds some extra features, more counters and flexibility. Dstat is handy for monitoring systems during performance tuning tests, benchmarks or troubleshooting. Dstat allows you to view all of your system resources instantly, you can eg. compare disk usage in combination with interrupts from your IDE controller, or compare the network bandwidth numbers directly with the disk throughput (in the same interval). Dstat gives you detailed selective information in columns and clearly indicates in what magnitude and unit the output is displayed. Less confusion, less mistakes.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dump-0.4b41-5.el5 - dump-0.4b41-6.el5

- Group: Applications/Archiving
- Summary: Programs for backing up and restoring ext2/ext3 filesystems
- Description: The dump package contains both dump and restore. Dump examines files in a filesystem, determines which ones need to be backed up, and copies those files to a specified disk, tape, or other storage medium. The restore command performs the inverse function of dump; it can restore a full backup of a filesystem. Subsequent incremental backups can then be layered on top of the full backup. Single files and directory subtrees may also be restored from full or partial backups. Install dump if you need a system for both backing up filesystems and restoring filesystems after backups.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ecryptfs-utils-75-5.el5 - ecryptfs-utils-75-8.el5

- Group: System Environment/Base
- Summary: The eCryptfs mount helper and support libraries
- Description: eCryptfs is a stacked cryptographic filesystem that ships in the Linux kernel. This package provides the mount helper and supporting libraries to perform key management and mount functions. Install ecryptfs-utils if you would like to mount eCryptfs.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

esound-0.2.36-3 - esound-0.2.36-4

- Group: System Environment/Daemons
- Summary: Allows several audio streams to play on a single audio device.
- Description: EsounD, the Enlightened Sound Daemon, is a server process that mixes several audio streams for playback by a single audio device. For example, if you're listening

to music on a CD and you receive a sound-related event from ICQ, the two applications won't have to queue for the use of your sound card. Install esound if you'd like to let sound applications share your audio device. You'll also need to install the audiofile package.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

evince-0.6.0-13.el5 - evince-0.6.0-17.el5

- Group: Applications/Publishing
- Summary: Document viewer
- Description: evince is a GNOME-based document viewer.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

expect-5.43.0-5.1 - expect-5.43.0-8.el5

- Group: Development/Languages
- Summary: A program-script interaction and testing utility
- Description: Expect is a tcl application for automating and testing interactive applications such as telnet, ftp, passwd, fsck, rlogin, tip, etc. Expect makes it easy for a script to control another program and interact with it. This package contains expect and some scripts that use it.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

fcoe-utils-1.0.7-4.el5 - fcoe-utils-1.0.7-5.el5

- Group: Applications/System

- Summary: Fibre Channel over Ethernet utilities
- Description: Fibre Channel over Ethernet utilities fcoeadm - command line tool for configuring FCoE interfaces fcoemon - service to configure DCB Ethernet QOS filters, works with dcbd
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

fetchmail-6.3.6-1.1.el5_3.1 - fetchmail-6.3.6-4.el5

- Group: Applications/Internet
- Summary: A remote mail retrieval and forwarding utility
- Description: Fetchmail is a remote mail retrieval and forwarding utility intended for use over on-demand TCP/IP links, like SLIP or PPP connections. Fetchmail supports every remote-mail protocol currently in use on the Internet (POP2, POP3, RPOP, APOP, KPOP, all IMAPs, ESMTP ETRN, IPv6, and IPSEC) for retrieval. Then Fetchmail forwards the mail through SMTP so you can read it through your favorite mail client. Install fetchmail if you need to retrieve mail over SLIP or PPP connections.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

file-4.17-15.el5_3.1 - file-4.17-21

- Group: Applications/File
- Summary: A utility for determining file types.
- Description: The file command is used to identify a particular file according to the type of data contained by the file. File can identify many different file types, including ELF binaries, system libraries, RPM packages, and different graphics formats. You should install the file package, since the file command is such a useful utility.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

firefox-3.6.18-1.el5_6 - firefox-3.6.26-1.el5_7

- Group: Applications/Internet
- Summary: Mozilla Firefox Web browser
- Description: Mozilla Firefox is an open-source web browser, designed for standards compliance, performance and portability.
- Added Dependencies:
  - xulrunner-devel >= 1.9.2.26-1
- Removed Dependencies:
  - xulrunner-devel >= 1.9.2.18-1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

firstboot-1.4.27.8-1.el5 - firstboot-1.4.27.9-1.el5

- Group: System Environment/Base
- Summary: Initial system configuration utility
- Description: The firstboot utility runs after installation. It guides the user through a series of steps that allows for easier configuration of the machine.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

foomatic-3.0.2-38.3.el5 - foomatic-3.0.2-38.3.el5_7.1

- Group: System Environment/Libraries
- Summary: Foomatic printer database.
- Description: Foomatic is a comprehensive, spooler-independent database of printers, printer drivers, and driver descriptions. It contains utilities to generate driver description files and printer queues for CUPS, LPD, LPRng, and PDQ using the database. There is also the possibility to read the PJL options out of PJL-capable laser printers and take them into account at the driver description file generation. There are spooler-independent command line interfaces to manipulate queues (foomatic-configure) and to print files/manipulate jobs (foomatic printjob). The site http://www.linuxprinting.org/ is based on this database.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

freeipmi-0.5.1-6.el5 - freeipmi-0.5.1-7.el5

- Group: Applications/System
- Summary: FreeIPMI
- Description: The FreeIPMI project provides "Remote-Console" (out-of-band) and "System Management Software" (in-band) based on Intelligent Platform Management Interface specification. This package contains a Technology Preview for FreeIPMI. Please visit http://www.redhat.com/support/service/ for details on the Red Hat support policies.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

freeradius2-2.1.7-7.el5 - freeradius2-2.1.12-3.el5

- Group: System Environment/Daemons
- Summary: High-performance and highly configurable free RADIUS server
- Description: The FreeRADIUS Server Project is a high performance and highly configurable GPL'd free RADIUS server. The server is similar in some respects to Livingston's 2.0 server. While FreeRADIUS started as a variant of the Cistron RADIUS server, they don't share a lot in common any more. It now has many more features than Cistron or Livingston, and is much more configurable. FreeRADIUS is an Internet authentication daemon, which implements the RADIUS protocol, as defined in RFC 2865 (and others). It allows Network Access Servers (NAS boxes) to perform authentication for dial-up users. There are also RADIUS clients available for Web servers, firewalls, Unix logins, and more. Using RADIUS allows authentication and authorization for a network to be centralized, and minimizes the amount of re-configuration which has to be done when adding or deleting new users.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

freetype-2.2.1-28.el5_5.1 - freetype-2.2.1-28.el5_7.2

- Group: System Environment/Libraries
- Summary: A free and portable font rendering engine
- Description: The FreeType engine is a free and portable font rendering engine, developed to provide advanced font support for a variety of platforms and environments. FreeType is a library which can open and manages font files as well as efficiently load, hint and render individual glyphs. FreeType is not a font server or a complete text-rendering library.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ftp-0.17-35.el5 - ftp-0.17-37.el5

- Group: Applications/Internet
- Summary: The standard UNIX FTP (File Transfer Protocol) client.
- Description: The ftp package provides the standard UNIX command-line FTP (File Transfer Protocol) client. FTP is a widely used protocol for transferring files over the Internet and for archiving files. If your system is on a network, you should install ftp in order to do file transfers.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gamin-0.1.7-8.el5 - gamin-0.1.7-10.el5

- Group: Development/Libraries
- Summary: Library providing the FAM File Alteration Monitor API
- Description: This C library provides an API and ABI compatible file alteration monitor mechanism compatible with FAM but not dependent on a system wide daemon.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

gawk-3.1.5-14.el5 - gawk-3.1.5-15.el5

- Group: Applications/Text
- Summary: The GNU version of the awk text processing utility.
- Description: The gawk packages contains the GNU version of awk, a text processing utility. Awk interprets a special-purpose programming language to do quick and easy text pattern matching and reformatting jobs. Install the gawk package if you need a text processing utility. Gawk is considered to be a standard Linux tool for processing text.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gcc-4.1.2-51.el5 - gcc-4.1.2-52.el5

- Group: Development/Languages
- Summary: Various compilers (C, C++, Objective-C, Java, ...)
- Description: The gcc package contains the GNU Compiler Collection version 4.1. You'll need this package in order to compile C code.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gcc44-4.4.4-13.el5 - gcc44-4.4.6-3.el5.1

- Group: Development/Languages
- Summary: Preview of GCC version 4.4
- Description: The gcc44 package contains preview of the GNU Compiler Collection version 4.4.
- Added Dependencies:
  - binutils220
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gdb-7.0.1-37.el5 - gdb-7.0.1-42.el5

- Group: Development/Debuggers
- Summary: A GNU source-level debugger for C, C++, Java and other languages
- Description: GDB, the GNU debugger, allows you to debug programs written in C, C++, Java, and other languages, by executing them in a controlled fashion and printing their data.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gdbm-1.8.0-26.2.1 - gdbm-1.8.0-26.2.1.el5_6.1

- Group: System Environment/Libraries
- Summary: A GNU set of database routines which use extensible hashing.
- Description: Gdbm is a GNU database indexing library, including routines which use extensible hashing. Gdbm works in a similar way to standard UNIX dbm routines. Gdbm is useful for developers who write C applications and need access to a simple and efficient database or who are building C applications which will use such a database. If you're a C developer and your programs need access to simple database routines, you should install gdbm. You'll also need to install gdbm-devel.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gdm-2.16.0-56.el5 - gdm-2.16.0-59.el5

- Group: User Interface/X
- Summary: The GNOME Display Manager.
- Description: Gdm (the GNOME Display Manager) is a highly configurable reimplementation of xdm, the X Display Manager. Gdm allows you to log into your system with the X Window System running and supports running several different X sessions on your local machine at the same time.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gfs-kmod-0.1.34-15.el5 - gfs-kmod-0.1.34-17.el5

- Group: System Environment/Kernel
- Summary: gfs kernel modules
- Description: gfs - The Global File System is a symmetric, shared-disk, cluster file system.
- Added Dependencies:
  - kernel-devel-ia64 = 2.6.18-302.el5
  - kernel-xen-devel-ia64 = 2.6.18-302.el5
- Removed Dependencies:
  - kernel-devel-ia64 = 2.6.18-223.el5
  - kernel-xen-devel-ia64 = 2.6.18-223.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gfs-utils-0.1.20-10.el5 - gfs-utils-0.1.20-13.el5

- Group: System Environment/Kernel
- Summary: Utilities for managing the global filesystem (GFS)
- Description: The gfs-utils package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in GFS filesystems.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gfs2-utils-0.1.62-31.el5 - gfs2-utils-0.1.62-34.el5

- Group: System Environment/Kernel

- Summary: Utilities for managing the global filesystem (GFS)
- Description: The gfs2-utils package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in GFS filesystems.
- Added Dependencies:
  - zlib-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ghostscript-8.70-6.el5 - ghostscript-8.70-14.el5

- Group: Applications/Publishing
- Summary: A PostScript(TM) interpreter and renderer.
- Description: Ghostscript is a set of software that provides a PostScript(TM) interpreter, a set of C procedures (the Ghostscript library, which implements the graphics capabilities in the PostScript language) and an interpreter for Portable Document Format (PDF) files. Ghostscript translates PostScript code into many common, bitmapped formats, like those understood by your printer or screen. Ghostscript is normally used to display PostScript files and to print PostScript files to non-PostScript printers. If you need to display PostScript files or print them to non-PostScript printers, you should install ghostscript. If you install ghostscript, you also need to install the ghostscript-fonts package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

glibc-2.5-65 - glibc-2.5-81

- Group: System Environment/Libraries
- Summary: The GNU libc libraries.
- Description: The glibc package contains standard libraries which are used by multiple programs on the system. In order to save disk space and memory, as well as to make upgrading easier, common system code is kept in one place and shared between programs. This particular package contains the most important sets of shared libraries: the standard C library and the standard math library. Without these two libraries, a Linux system will not function.
- Added Dependencies:
  - systemtap-sdt-devel
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gnome-screensaver-2.16.1-8.el5_6.3 - gnome-screensaver-2.16.1-8.el5_7.5

- Group: Amusements/Graphics
- Summary: GNOME Screensaver
- Description: gnome-screensaver is a screen saver and locker that aims to have simple, sane, secure defaults and be well integrated with the desktop.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gnome-system-monitor-2.16.0-3.el5 - gnome-system-monitor-2.16.0-4.el5

- Group: Applications/System
- Summary: Simple process monitor
- Description: gnome-system-monitor is a simple process and system monitor.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gpart-0.1h-5.el5 - gpart-0.1h-6.el5

- Group: Applications/System
- Summary: A program for recovering corrupt partition tables
- Description: Gpart is a small tool which tries to guess what partitions are on a PC type harddisk in case the primary partition table was damaged.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

groff-1.18.1.1-11.1 - groff-1.18.1.1-13.el5

- Group: Applications/Publishing
- Summary: A document formatting system.
- Description: Groff is a document formatting system. Groff takes standard text and formatting commands as input and produces formatted output. The created documents can be shown on a display or printed on a printer. Groff's formatting commands allow you to specify font type and size, bold type, italic type, the number and size of columns on a page, and more. Groff can also be used to format man pages. If you are going to use groff with the X Window System, you will also need to install the groff-gxditview package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gtk2-2.10.4-21.el5_5.6 - gtk2-2.10.4-21.el5_7.7

- Group: System Environment/Libraries
- Summary: The GIMP ToolKit (GTK+), a library for creating GUIs for X
- Description: GTK+ is a multi-platform toolkit for creating graphical user interfaces. Offering a complete set of widgets, GTK+ is suitable for projects ranging from small one-off tools to complete application suites.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

hmaccalc-0.9.6-3.el5 - hmaccalc-0.9.6-4.el5

- Group: System Environment/Base
- Summary: Tools for computing and checking HMAC values for files
- Description: The hmaccalc package contains tools which can calculate HMAC (hash-based message authentication code) values for files. The names and interfaces are meant to mimic the sha*sum tools provided by the coreutils package.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

httpd-2.2.3-53.el5 - httpd-2.2.3-63.el5

- Group: System Environment/Daemons
- Summary: Apache HTTP Server
- Description: The Apache HTTP Server is a powerful, efficient, and extensible web server.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

hwdata-0.213.24-1.el5 - hwdata-0.213.26-1.el5

- Group: System Environment/Base
- Summary: Hardware identification and configuration data
- Description: hwdata contains various hardware identification and configuration data, such as the pci.ids database and MonitorsDb databases.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ibutils-1.2-11.el5 - ibutils-1.2-11.2.el5

- Group: System Environment/Libraries
- Summary: OpenIB Mellanox InfiniBand Diagnostic Tools
- Description: ibutils provides IB network and path diagnostics.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

icu-3.6-5.16 - icu-3.6-5.16.1

- Group: System Environment/Libraries
- Summary: International Components for Unicode
- Description: The International Components for Unicode (ICU) libraries provide robust and full-featured Unicode services on a wide variety of platforms. ICU supports the most current version of the Unicode standard, and they provide support for supplementary Unicode characters (needed for GB 18030 repertoire support). As computing environments become more heterogeneous, software portability becomes more important. ICU lets you produce the same results across all the various platforms you support, without sacrificing performance. It offers great flexibility to extend and customize the supplied services.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ifd-egate-0.05-15 - ifd-egate-0.05-17.el5

- Group: System Environment/Base
- Summary: Axalto Egate SmartCard device driver for PCSC-lite
- Description: The Axalto Egate device driver enables PCSC-lite to communicate with Axalto Egate cards, which CoolKey is based off of.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

initscripts-8.45.38-2.el5 - initscripts-8.45.42-1.el5

- Group: System Environment/Base
- Summary: The inittab file and the /etc/init.d scripts.

- Description: The initscripts package contains the basic system scripts used to boot your Red Hat system, change runlevels, and shut the system down cleanly. Initscripts also contains the scripts that activate and deactivate most network interfaces.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ipa-client-2.0-14.el5 - ipa-client-2.1.3-1.el5

- Group: System Environment/Base
- Summary: IPA authentication for use on clients
- Description: IPA is an integrated solution to provide centrally managed Identity (machine, user, virtual machines, groups, authentication credentials), Policy (configuration settings, access control information) and Audit (events, logs, analysis thereof).
- Added Dependencies:
  - curl-devel >= 7.15.5-9.el5_7.4
  - xmlrpc-c-devel >= 1.16.24-1206.1840.el5_7.3
- Removed Dependencies:
  - curl-devel
  - xmlrpc-c-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iproute-2.6.18-11.el5 - iproute-2.6.18-13.el5

- Group: Applications/System
- Summary: Advanced IP routing and network device configuration tools.
- Description: The iproute package contains networking utilities (ip and rtmon, for example) which are designed to use the advanced networking capabilities of the Linux 2.4.x and 2.6.x kernel.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

iprutils-2.3.4-1.el5 - iprutils-2.3.7-2.el5

- Group: System Environment/Base
- Summary: Utilities for the IBM Power Linux RAID adapters
- Description: Provides a suite of utilities to manage and configure SCSI devices supported by the ipr SCSI storage device driver.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iptables-1.3.5-5.3.el5_4.1 - iptables-1.3.5-9.1.el5

- Group: System Environment/Base
- Summary: Tools for managing Linux kernel packet filtering capabilities.
- Description: The iptables utility controls the network packet filtering code in the Linux kernel. If you need to set up firewalls and/or IP masquerading, you should install this package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iscsi-initiator-utils-6.2.0.872-10.el5 - iscsi-initiator-utils-6.2.0.872-13.el5

- Group: System Environment/Daemons
- Summary: iSCSI daemon and utility programs
- Description: The iscsi package provides the server daemon for the iSCSI protocol, as well as the utility programs used to manage it. iSCSI is a protocol for distributed disk access using SCSI commands sent over Internet Protocol networks.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

java-1.6.0-openjdk-1.6.0.0-1.22.1.9.8.el5_6 - java-1.6.0-openjdk-1.6.0.0-1.24.1.10.4.el5

- Group: Development/Languages
- Summary: OpenJDK Runtime Environment
- Description: The OpenJDK runtime environment.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kdeadmin-3.5.4-3.el5 - kdeadmin-3.5.4-4.el5

- Group: User Interface/Desktops
- Summary: Administrative tools for KDE.
- Description: The kdeadmin package includes administrative tools for the K Desktop Environment (KDE) including: kcron - Crontab editor kdat - Tape backup tool kuser - Frontend for configuring users and user groups
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kdebase-3.5.4-24.el5 - kdebase-3.5.4-25.el5

- Group: User Interface/Desktops
- Summary: K Desktop Environment - core files
- Description: Core applications for the K Desktop Environment. Included are: kdm (replacement for xdm), kwin (window manager), konqueror (filemanager, web browser, ftp client, ...), konsole (xterm replacement), kpanel (application starter and desktop pager), kaudio (audio server), kdehelp (viewer for kde help files, info and man pages), kthememgr (system for managing alternate theme packages) plus other KDE components (kcheckpass, kikbd, kscreensaver, kcontrol, kfind, kfontmanager, kmenuedit).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kdelibs-3.5.4-25.el5_4.1 - kdelibs-3.5.4-26.el5_7.1

- Group: System Environment/Libraries
- Summary: K Desktop Environment - Libraries
- Description: Libraries for the K Desktop Environment: KDE Libraries included: kdecore (KDE core library), kdeui (user interface), kfm (file manager), khtmlw (HTML widget), kio (Input/Output, networking), kspell (spelling checker), jscript (javascript), kab (addressbook), kimgio (image manipulation).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kdeutils-3.5.4-5.fc6 - kdeutils-3.5.4-6.el5

- Group: Applications/System
- Summary: K Desktop Environment - Utilities
- Description: Utilities for the K Desktop Environment. Includes: ark (tar/gzip archive manager); kcalc (scientific calculator); kcharselect (character selector); kdepasswd (change password); kdessh (ssh front end); kdf (view disk usage); kedit (simple text editor); kfloppy (floppy formatting tool); khexedit (hex editor); kjots (note taker); klaptopdaemon (battery monitoring and management for laptops); ksim (system information monitor); ktimer (task scheduler); kwikdisk (removable media utility)
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kernel-2.6.18-274.el5 - kernel-2.6.18-308.el5

- Group: System Environment/Kernel
- Summary: The Linux kernel (the core of the Linux operating system)
- Description: The kernel package contains the Linux kernel (vmlinuz), the core of any Linux operating system. The kernel handles the basic functions of the operating system: memory

allocation, process allocation, device input and output, etc.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kexec-tools-1.102pre-126.el5_6.6 - kexec-tools-1.102pre-154.el5

- Group: Applications/System
- Summary: The kexec/kdump userspace component.
- Description: kexec-tools provides /sbin/kexec binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. This package contains the /sbin/kexec binary and ancillary utilities that together form the userspace component of the kernel's kexec feature.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

krb5-1.6.1-62.el5 - krb5-1.6.1-70.el5

- Group: System Environment/Libraries
- Summary: The Kerberos network authentication system.
- Description: Kerberos V5 is a trusted-third-party network authentication system, which can improve your network's security by eliminating the insecure practice of cleartext passwords.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ksh-20100202-1.el5_6.6 - ksh-20100621-5.el5

- Group: Applications/Shells
- Summary: The Original ATT Korn Shell

- Description: KSH-93 is the most recent version of the KornShell by David Korn of AT&T Bell Laboratories. KornShell is a shell programming language, which is upward compatible with "sh" (the Bourne Shell).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kudzu-1.2.57.1.26-1 - kudzu-1.2.57.1.26-3

- Group: Applications/System
- Summary: The Red Hat Linux hardware probing tool.
- Description: Kudzu is a hardware probing tool run at system boot time to determine what hardware has been added or removed from the system.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kvm-83-239.el5 - kvm-83-249.el5

- Group: Development/Tools
- Summary: Kernel-based Virtual Machine
- Description: KVM (for Kernel-based Virtual Machine) is a full virtualization solution for Linux on x86 hardware. Using KVM, one can run multiple virtual machines running unmodified Linux or Windows images. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, etc.
- Added Dependencies:
  - kernel-debug-devel = 2.6.18-304.el5
  - kernel-devel = 2.6.18-304.el5
- Removed Dependencies:
  - kernel-debug-devel = 2.6.18-269.el5
  - kernel-devel = 2.6.18-269.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

less-436-7.el5 - less-436-9.el5

- Group: Applications/Text
- Summary: A text file browser similar to more, but better.
- Description: The less utility is a text file browser that resembles more, but has more capabilities. Less allows you to move backwards in the file as well as forwards. Since less doesn't have to read the entire input file before it starts, less starts up more quickly than text editors (for example, vi). You should install less because it is a basic utility for viewing text files, and you'll use it frequently.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lftp-3.7.11-4.el5_5.3 - lftp-3.7.11-7.el5

- Group: Applications/Internet
- Summary: A sophisticated file transfer program
- Description: LFTP is a sophisticated ftp/http file transfer program. Like bash, it has job control and uses the readline library for input. It has bookmarks, built-in mirroring, and can transfer several files in parallel. It is designed with reliability in mind.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libX11-1.0.3-11.el5 - libX11-1.0.3-11.el5_7.1

- Group: System Environment/Libraries
- Summary: X.Org X11 libX11 runtime library
- Description: X.Org X11 libX11 runtime library
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

libXcursor-1.1.7-1.1 - libXcursor-1.1.7-1.2

- Group: System Environment/Libraries
- Summary: X.Org X11 libXcursor runtime library
- Description: X.Org X11 libXcursor runtime library
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libXfont-1.2.2-1.0.3.el5_1 - libXfont-1.2.2-1.0.4.el5_7

- Group: System Environment/Libraries
- Summary: X.Org X11 libXfont runtime library
- Description: X.Org X11 libXfont runtime library
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libcxgb3-1.2.5-2.el5 - libcxgb3-1.3.0-1.el5

- Group: System Environment/Libraries
- Summary: Chelsio T3 iWARP HCA Userspace Driver
- Description: Userspace hardware driver for use with the libibverbs InfiniBand/iWARP verbs library. This driver enables Chelsio iWARP capable ethernet devices.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

libdhcp-1.20-11.el5 - libdhcp-1.20-13.el5

- Group: Development/Libraries
- Summary: A library for network interface configuration with DHCP
- Description: libdhcp enables programs to invoke and control the Dynamic Host Configuration Protocol (DHCP) clients: the Internet Software Consortium (ISC) IPv4 DHCP client library, libdhcp4client, and the IPv6 DHCPv6 client library, libdhcp6client, and provides Network Interface Configuration (NIC) services for network parameter autoconfiguration with DHCP.
- Added Dependencies:
  - dhcp-devel >= 12:3.0.5-31
  - libdhcp4client-devel >= 12:3.0.5-31
- Removed Dependencies:
  - dhcp-devel >= 12:3.0.5-26
  - libdhcp4client-devel >= 12:3.0.5-26
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libexif-0.6.13-4.0.2.el5_1.1 - libexif-0.6.20-1.el5_7.1

- Group: System Environment/Libraries
- Summary: Library for extracting extra information from image files
- Description: Most digital cameras produce EXIF files, which are JPEG files with extra tags that contain information about the image. The EXIF library allows you to parse an EXIF file and read the data from those tags.
- Added Dependencies:
  - pkgconfig
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libhbaapi-2.2-4.el5 - libhbaapi-2.2-6.el5

- Group: System Environment/Libraries
- Summary: SNIA HBAAPI library
- Description: The SNIA HBA API library. C-level project to manage Fibre Channel Host Bus Adapters.

- Added Dependencies:
  - autoconf
  - libtool
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libmlx4-1.0.1-6.el5 - libmlx4-1.0.1-7.el5

- Group: System Environment/Libraries
- Summary: Mellanox ConnectX InfiniBand HCA Userspace Driver
- Description: Mellanox hardware driver for use with libibverbs user space verbs access library. This driver supports Mellanox ConnectX architecture cards.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libpng-1.2.10-7.1.el5_5.3 - libpng-1.2.10-7.1.el5_7.5

- Group: System Environment/Libraries
- Summary: A library of functions for manipulating PNG image format files
- Description: The libpng package contains a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files. PNG is a bit-mapped graphics format similar to the GIF format. PNG was created to replace the GIF format, since GIF uses a patented data compression algorithm. Libpng should be installed if you need to manipulate PNG format image files.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libusb-0.1.12-5.1 - libusb-0.1.12-6.el5

- Group: System Environment/Libraries
- Summary: A library which allows userspace access to USB devices.
- Description: This package provides a way for applications to access USB devices.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libvirt-0.8.2-22.el5 - libvirt-0.8.2-25.el5

- Group: Development/Libraries
- Summary: Library providing a simple API virtualization
- Description: Libvirt is a C toolkit to interact with the virtualization capabilities of recent versions of Linux (and other OSes).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libxml2-2.6.26-2.1.12 - libxml2-2.6.26-2.1.12.el5_7.2

- Group: Development/Libraries
- Summary: Library providing XML and HTML support
- Description: This library allows to manipulate XML files. It includes support to read, modify and write XML and HTML files. There is DTDs support this includes parsing and validation even with complex DtDs, either at parse time or later once the document has been modified. The output can be a simple SAX stream or and in-memory DOM like representations. In this case one can use the built-in XPath and XPointer implementation to select subnodes or ranges. A flexible Input/Output mechanism is available, with existing HTTP and FTP modules and combined to an URI library.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lsof-4.78-3 - lsof-4.78-6

- Group: Development/Debuggers
- Summary: A utility which lists open files on a Linux/UNIX system.
- Description: Lsof stands for LiSt Open Files, and it does just that: it lists information about files that are open by the processes running on a UNIX system.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ltrace-0.5-13.45svn.el5 - ltrace-0.5-13.45svn.el5_7.12

- Group: Development/Debuggers
- Summary: Tracks runtime library calls from dynamically linked executables.
- Description: Ltrace is a debugging program which runs a specified command until the command exits. While the command is executing, ltrace intercepts and records both the dynamic library calls called by the executed process and the signals received by the executed process. Ltrace can also intercept and print system calls executed by the process. You should install ltrace if you need a sysadmin tool for tracking the execution of processes.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lvm2-2.02.84-6.el5 - lvm2-2.02.88-7.el5

- Group: System Environment/Base
- Summary: Userland logical volume management tools
- Description: LVM2 includes all of the support for handling read/write operations on physical volumes (hard disks, RAID-Systems, magneto optical, etc., multiple devices (MD), see mdadd(8) or even loop devices, see losetup(8)), creating volume groups (kind of virtual disks) from one or more physical volumes and creating one or more logical volumes (kind of logical partitions) in volume groups.
- Added Dependencies:
  - device-mapper >= 1.02.67-2
- Removed Dependencies:
  - device-mapper >= 1.02.63-2

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lvm2-cluster-2.02.84-6.el5 - lvm2-cluster-2.02.88-7.el5

- Group: System Environment/Base
- Summary: Cluster extensions for userland logical volume management tools
- Description: Extensions to LVM2 to support clusters.
- Added Dependencies:
  - device-mapper >= 1.02.67-2
- Removed Dependencies:
  - device-mapper >= 1.02.63-2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

man-pages-2.39-17.el5 - man-pages-2.39-20.el5

- Group: Documentation
- Summary: Man (manual) pages from the Linux Documentation Project.
- Description: A large collection of man pages (documentation) from the Linux Documentation Project (LDP).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

man-pages-ja-20060815-14.el5 - man-pages-ja-20060815-15.el5

- Group: Documentation
- Summary: Japanese man (manual) pages from the Japanese Manual Project
- Description: Japanese Manual pages, translated by JM-Project (Japanese Manual Project).
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

man-pages-overrides-0.5.7.3-3.el5 - man-pages-overrides-5.8.3-2.el5

- Group: Documentation
- Summary: Complementary and updated manual pages
- Description: A collection of manual ("man") pages to complement other packages or update those contained therein. Always have the latest version of this package installed.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mesa-6.5.1-7.8.el5 - mesa-6.5.1-7.10.el5

- Group: System Environment/Libraries
- Summary: Mesa graphics libraries
- Description: Mesa
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

microcode_ctl-1.17-1.52.el5 - microcode_ctl-1.17-1.56.el5

- Group: System Environment/Base
- Summary: Tool to update x86/x86-64 CPU microcode.
- Description: microcode_ctl - updates the microcode on Intel x86/x86-64 CPU's
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mkinitrd-5.1.19.6-71.el5 - mkinitrd-5.1.19.6-75.el5

- Group: System Environment/Base
- Summary: Creates an initial ramdisk image for preloading modules.
- Description: Mkinitrd creates filesystem images for use as initial ramdisk (initrd) images. These ramdisk images are often used to preload the block device modules (SCSI or RAID) needed to access the root filesystem. In other words, generic kernels can be built without drivers for any SCSI adapters which load the SCSI driver as a module. Since the kernel needs to read those modules, but in this case it isn't able to address the SCSI adapter, an initial ramdisk is used. The initial ramdisk is loaded by the operating system loader (normally LILO) and is available to the kernel as soon as the ramdisk is loaded. The ramdisk image loads the proper SCSI adapter and allows the kernel to mount the root filesystem. The mkinitrd program creates such a ramdisk using information found in the /etc/modules.conf file.
- Added Dependencies:
  - libdhcp-devel >= 1.20-12
- Removed Dependencies:
  - libdhcp-devel >= 1.20-6
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mktemp-1.5-23.2.2 - mktemp-1.5-24.el5

- Group: System Environment/Base
- Summary: A small utility for safely making /tmp files.
- Description: The mktemp utility takes a given file name template and overwrites a portion of it to create a unique file name. This allows shell scripts and other programs to safely create and use /tmp files. Install the mktemp package if you need to use shell scripts or other programs which will create and use unique /tmp files.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mod_auth_kerb-5.1-3.el5 - mod_auth_kerb-5.1-3.el5_7.1

- Group: System Environment/Daemons
- Summary: Kerberos authentication module for HTTP
- Description: mod_auth_kerb is module for the Apache HTTP Server designed to provide Kerberos authentication over HTTP. The module supports the Negotiate authentication method, which performs full Kerberos authentication based on ticket exchanges.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mod_revocator-1.0.3-5.el5 - mod_revocator-1.0.3-9.el5

- Group: System Environment/Daemons
- Summary: CRL retrieval module for the Apache HTTP server
- Description: The mod_revocator module retrieves and installs remote Certificate Revocate Lists (CRLs) into an Apache web server.
- Added Dependencies:
  - autoconf
  - libtool
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mrtg-2.14.5-2 - mrtg-2.14.5-4.el5

- Group: Applications/Internet
- Summary: Multi Router Traffic Grapher
- Description: The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network-links. MRTG generates HTML pages containing PNG images which provide a LIVE visual representation of this traffic.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

mysql-connector-odbc-3.51.26r1127-1.el5 - mysql-connector-odbc-3.51.26r1127-2.el5

- Group: System Environment/Libraries
- Summary: ODBC driver for MySQL
- Description: An ODBC (rev 3) driver for MySQL, for use with unixODBC.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

net-snmp-5.3.2.2-14.el5 - net-snmp-5.3.2.2-17.el5

- Group: System Environment/Daemons
- Summary: A collection of SNMP protocol tools and libraries.
- Description: SNMP (Simple Network Management Protocol) is a protocol used for network management. The NET-SNMP project includes various SNMP tools: an extensible agent, an SNMP library, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps, a version of the netstat command which uses SNMP, and a Tk/Perl mib browser. This package contains the snmpd and snmptrapd daemons, documentation, etc. You will probably also want to install the net-snmp-utils package, which contains NET-SNMP utilities. Building option: --without tcp_wrappers : disable tcp_wrappers support
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

net-tools-1.60-81.el5 - net-tools-1.60-82.el5

- Group: System Environment/Base
- Summary: Basic networking tools.
- Description: The net-tools package contains basic networking tools, including ifconfig, netstat, route, and others.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

netpbm-10.35.58-8.el5 - netpbm-10.35.58-10.el5

- Group: System Environment/Libraries
- Summary: A library for handling different graphics file formats
- Description: The netpbm package contains a library of functions which support programs for handling various graphics file formats, including .pbm (portable bitmaps), .pgm (portable graymaps), .pnm (portable anymaps), .ppm (portable pixmaps) and others.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nfs-utils-1.0.9-54.el5 - nfs-utils-1.0.9-60.el5

- Group: System Environment/Daemons
- Summary: NFS utilities and supporting clients and daemons for the kernel NFS server.
- Description: The nfs-utils package provides a daemon for the kernel NFS server and related tools, which provides a much higher level of performance than the traditional Linux NFS server used by most users. This package also contains the showmount program. Showmount queries the mount daemon on a remote host for information about the NFS (Network File System) server on the remote host. For example, showmount can display the clients which are mounted on that host. This package also contains the mount.nfs and umount.nfs program.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nfs-utils-lib-1.0.8-7.6.el5 - nfs-utils-lib-1.0.8-7.9.el5

- Group: System Environment/Libraries
- Summary: Network File System Support Library

- Description: Support libraries that are needed by the commands and daemons the nfs-utils rpm.
- Added Dependencies:
  - libtool
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nfs4-acl-tools-0.3.3-1.el5 - nfs4-acl-tools-0.3.3-3.el5

- Group: System Environment/Tools
- Summary: The nfs4 ACL tools
- Description: This package contains commandline and GUI ACL utilities for the Linux NFSv4 client.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nmap-4.11-1.1 - nmap-4.11-2

- Group: Applications/System
- Summary: Network exploration tool and security scanner
- Description: Nmap is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many port scanning techniques (determine what services the hosts are offering), and TCP/IP fingerprinting (remote host operating system identification). Nmap also offers flexible target and port specification, decoy scanning, determination of TCP sequence predictability characteristics, reverse-identd scanning, and more.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nspr-4.8.6-1.el5 - nspr-4.8.8-2.el5

- Group: System Environment/Libraries
- Summary: Netscape Portable Runtime
- Description: NSPR provides platform independence for non-GUI operating system facilities. These facilities include threads, thread synchronization, normal file and network I/O, interval timing and calendar time, basic memory management (malloc and free) and shared library linking.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nss-3.12.8-4.el5_6 - nss-3.12.10-8.el5

- Group: System Environment/Libraries
- Summary: Network Security Services
- Description: Network Security Services (NSS) is a set of libraries designed to support cross-platform development of security-enabled client and server applications. Applications built with NSS can support SSL v2 and v3, TLS, PKCS #5, PKCS #7, PKCS #11, PKCS #12, S/MIME, X.509 v3 certificates, and other security standards.
- Added Dependencies:
  - nspr-devel >= 4.8.8
- Removed Dependencies:
  - nspr-devel >= 4.8.6
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nss_ldap-253-42.el5 - nss_ldap-253-49.el5

- Group: System Environment/Base
- Summary: NSS library and PAM module for LDAP.
- Description: This package includes two LDAP access clients: nss_ldap and pam_ldap. Nss_ldap is a set of C library extensions that allow X.500 and LDAP directory servers to be used as a primary source of aliases, ethers, groups, hosts, networks, protocol, users, RPCs, services, and shadow passwords (instead of or in addition to using flat files or NIS). Pam_ldap is a module for Linux-PAM that supports password changes, V2 clients, Netscape's SSL, ypldapd, Netscape Directory Server password policies, access authorization, and crypted hashes.

- Added Dependencies:
  - openldap-devel >= 2.3.43-20
- Removed Dependencies:
  - openldap-devel >= 2.3.43-7
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ntp-4.2.2p1-15.el5 - ntp-4.2.2p1-15.el5_7.1

- Group: System Environment/Daemons
- Summary: Synchronizes system time using the Network Time Protocol (NTP).
- Description: The Network Time Protocol (NTP) is used to synchronize a computer's time with another reference time source. The ntp package contains utilities and daemons that will synchronize your computer's time to Coordinated Universal Time (UTC) via the NTP protocol and NTP servers. The ntp package includes ntpdate (a program for retrieving the date and time from remote machines via a network) and ntpd (a daemon which continuously adjusts system time). Install the ntp package if you need tools for keeping your system's time synchronized via the NTP protocol.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

oddjob-0.27-11.el5 - oddjob-0.27-12.el5

- Group: System Environment/Daemons
- Summary: A D-BUS service which runs odd jobs on behalf of client applications
- Description: oddjob is a D-BUS service which performs particular tasks for clients which connect to it and issue requests using the system-wide message bus.
- Added Dependencies:
  - autoconf
  - automake
  - libtool
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

openCryptoki-2.2.4-22.el5_5.1 - openCryptoki-2.2.4-25.el5

- Group: Productivity/Security
- Summary: Implementation of Cryptoki v2.11 for IBM Crypto Hardware
- Description: The PKCS#11 Version 2.11 api implemented for the IBM Crypto cards. This package includes support for the IBM 4758 Cryptographic CoProcessor (with the PKCS#11 firmware loaded) and the IBM eServer Cryptographic Accelerator (FC 4960 on pSeries)
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openais-0.80.6-30.el5 - openais-0.80.6-36.el5

- Group: System Environment/Base
- Summary: The openais Standards-Based Cluster Framework executive and APIs
- Description: This package contains the openais executive, openais service handlers, default configuration files and init script.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openldap-2.3.43-12.el5_6.7 - openldap-2.3.43-25.el5

- Group: System Environment/Daemons
- Summary: The configuration files, libraries, and documentation for OpenLDAP.
- Description: OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. LDAP is a set of protocols for accessing directory services (usually phone book style information, but other information is possible) over the Internet, similar to the way DNS (Domain Name System) information is propagated over the Internet. The openldap package contains configuration files, libraries, and documentation for OpenLDAP.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openmotif-2.3.1-5.el5_5.1 - openmotif-2.3.1-6.el5

- Group: System Environment/Libraries
- Summary: Open Motif runtime libraries and executables.
- Description: This is the Open Motif 2.3.1 runtime environment. It includes the Motif shared libraries, needed to run applications which are dynamically linked against Motif, and the Motif Window Manager "mwm".
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openmotif22-2.2.3-18 - openmotif22-2.2.3-20

- Group: System Environment/Libraries
- Summary: Open Motif runtime libraries and executables
- Description: This is the Open Motif 2.2.3 runtime environment. It includes the Motif shared libraries, needed to run applications which are dynamically linked against Motif.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openscap-0.7.2-1.el5 - openscap-0.8.0-1.el5

- Group: System Environment/Libraries
- Summary: Set of open source libraries enabling integration of the SCAP line of standards
- Description: OpenSCAP is a set of open source libraries providing an easier path for integration of the SCAP line of standards. SCAP is a line of standards managed by NIST with the goal of providing a standard language for the expression of Computer Network Defense related information.
- Added Dependencies:

    - GConf2-devel
    - libcap-devel
    - libnl-devel
    - libselinux-devel
    - openldap-devel
- Removed Dependencies:
    - curl-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openssh-4.3p2-72.el5_6.3 - openssh-4.3p2-82.el5

- Group: Applications/Internet
- Summary: The OpenSSH implementation of SSH protocol versions 1 and 2
- Description: SSH (Secure SHell) is a program for logging into and executing commands on a remote machine. SSH is intended to replace rlogin and rsh, and to provide secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel. OpenSSH is OpenBSD's version of the last free version of SSH, bringing it up to date in terms of security and features, as well as removing all patented algorithms to separate libraries. This package includes the core files necessary for both the OpenSSH client and server. To make this package useful, you should also install openssh-clients, openssh-server, or both.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openssl-0.9.8e-20.el5 - openssl-0.9.8e-22.el5

- Group: System Environment/Libraries
- Summary: The OpenSSL toolkit
- Description: The OpenSSL toolkit provides support for secure communications between machines. OpenSSL includes a certificate management tool and shared libraries which provide various cryptographic algorithms and protocols.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openswan-2.6.21-5.el5_6.4 - openswan-2.6.32-3.el5

- Group: System Environment/Daemons
- Summary: IPSEC implementation with IKEv1 and IKEv2 keying protocols
- Description: Openswan is a free implementation of IPsec & IKE for Linux. IPsec is the Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks. Everything passing through the untrusted net is encrypted by the ipsec gateway machine and decrypted by the gateway at the other end of the tunnel. The resulting tunnel is a virtual private network or VPN. This package contains the daemons and userland tools for setting up Openswan. It supports the NETKEY/XFRM IPsec kernel stack that exists in the default Linux kernel. Openswan 2.6.x also supports IKEv2 (RFC4306)
- Added Dependencies:
  - curl-devel
  - libselinux-devel
  - openldap-devel
- Removed Dependencies:
  - man
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

oprofile-0.9.4-15.el5 - oprofile-0.9.4-20.el5

- Group: Development/System
- Summary: System wide profiler
- Description: OProfile is a profiling system for systems running Linux. The profiling runs transparently during the background, and profile data can be collected at any time. OProfile makes use of the hardware performance counters provided on Intel P6, and AMD Athlon family processors, and can use the RTC for profiling on other x86 processor types. See the HTML documentation for further details.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pam_krb5-2.2.14-21.el5 - pam_krb5-2.2.14-22.el5

- Group: System Environment/Base
- Summary: A Pluggable Authentication Module for Kerberos 5.
- Description: This is pam_krb5, a pluggable authentication module that can be used with Linux-PAM and Kerberos 5. This module supports password checking, ticket creation, and optional TGT verification and conversion to Kerberos IV tickets. The included pam_krb5afs module also gets AFS tokens if so configured.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pam_pkcs11-0.5.3-23 - pam_pkcs11-0.5.3-26.el5

- Group: System Environment/Base
- Summary: PKCS #11/NSS PAM login module
- Description: This Linux-PAM login module allows a X.509 certificate based user authentication. The certificate and its dedicated private key are thereby accessed by means of an appropriate PKCS #11 module. For the verification of the users' certificates, locally stored CA certificates as well as either online or locally accessible CRLs and OCSP are used. This version uses NSS to validate the Certificates and manage the PKCS #11 smartCards. Additional included pam_pkcs11 related tools - pkcs11_eventmgr: Generate actions on card insert/removal/timeout events - pklogin_finder: Get the loginname that maps to a certificate - pkcs11_inspect: Inspect the contents of a certificate
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pango-1.14.9-8.el5_6.2 - pango-1.14.9-8.el5_7.3

- Group: System Environment/Libraries
- Summary: System for layout and rendering of internationalized text
- Description: Pango is a system for layout and rendering of internationalized text.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

parted-1.8.1-28.el5 - parted-1.8.1-29.el5

- Group: Applications/System
- Summary: The GNU disk partition manipulation program
- Description: The GNU Parted program allows you to create, destroy, resize, move, and copy hard disk partitions. Parted can be used for creating space for new operating systems, reorganizing disk usage, and copying data to new hard disks.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pciutils-3.1.7-3.el5 - pciutils-3.1.7-5.el5

- Group: Applications/System
- Summary: PCI bus related utilities
- Description: The pciutils package contains various utilities for inspecting and setting devices connected to the PCI bus. The utilities provided require kernel version 2.1.82 or newer (which support the /proc/bus/pci interface).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pdksh-5.2.14-36.el5 - pdksh-5.2.14-37.el5

- Group: System Environment/Shells
- Summary: A public domain shell implementing ksh-88
- Description: The pdksh package contains public domain implementation of ksh-88. The ksh shell is a command interpreter intended for both interactive and shell script use. Ksh's command language is a superset of the sh shell language. Pdksh is unmaintained since 1998 and is obsoleted by ksh package.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

perl-5.8.8-32.el5_6.3 - perl-5.8.8-38.el5

- Group: Development/Languages
- Summary: The Perl programming language
- Description: Perl is a high-level programming language with roots in C, sed, awk and shell scripting. Perl is good at handling processes and files, and is especially good at handling text. Perl's hallmarks are practicality and efficiency. While it is used to do a lot of different things, Perl's most common applications are system administration utilities and web programming. A large proportion of the CGI scripts on the web are written in Perl. You need the perl package installed on your system so that your system can handle Perl scripts. Install this package if you want to program in Perl or enable your system to handle Perl scripts.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

perl-XML-SAX-0.14-8 - perl-XML-SAX-0.14-11

- Group: Development/Libraries
- Summary: XML-SAX Perl module
- Description: XML-SAX Perl module.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

php-5.1.6-27.el5_5.3 - php-5.1.6-32.el5

- Group: Development/Languages
- Summary: The PHP HTML-embedded scripting language. (PHP: Hypertext Preprocessor)
- Description: PHP is an HTML-embedded scripting language that allows developers to write dynamically generated web pages. PHP is ideal for writing database-enabled websites, with built-in integration for several commercial and non-commercial database management systems. PHP is often used as a replacement for CGI scripts. The php package contains a module that adds support for the PHP language to the Apache HTTP Server.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

php-pear-1.4.9-6.el5 - php-pear-1.4.9-8.el5

- Group: System
- Summary: PHP Extension and Application Repository framework
- Description: PEAR is a framework and distribution system for reusable PHP components. This package contains the basic PEAR components.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

php53-5.3.3-1.el5_6.1 - php53-5.3.3-5.el5

- Group: Development/Languages
- Summary: PHP scripting language for creating dynamic web sites
- Description: PHP is an HTML-embedded scripting language. PHP attempts to make it easy for developers to write dynamically generated webpages. PHP also offers built-in database integration for several commercial and non-commercial database management systems, so writing a database-enabled webpage with PHP is fairly simple. The most common use of PHP coding is probably as a replacement for CGI scripts. The php package contains the module which adds support for the PHP language to Apache HTTP Server.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

piranha-0.8.4-22.el5 - piranha-0.8.4-24.el5

- Group: System Environment/Base
- Summary: Cluster administation tools
- Description: Various tools to administer and configure the Linux Virtual Server as well as heartbeating and failover components. The LVS is a dynamically adjusted kernel routing mechanism that provides load balancing primarily for web and ftp servers though other services are supported.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

poppler-0.5.4-4.4.el5_6.17 - poppler-0.5.4-19.el5

- Group: Development/Libraries
- Summary: PDF rendering library
- Description: Poppler, a PDF rendering library, it's a fork of the xpdf PDF viewer developed by Derek Noonburg of Glyph and Cog, LLC.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

postgresql-8.1.23-1.el5_6.1 - postgresql-8.1.23-1.el5_7.3

- Group: Applications/Databases
- Summary: PostgreSQL client programs and libraries.
- Description: PostgreSQL is an advanced Object-Relational database management system (DBMS) that supports almost all SQL constructs (including transactions, subselects and user-defined types and functions). The postgresql package includes the client programs and libraries that you'll need to access a PostgreSQL DBMS server. These PostgreSQL client programs are programs that directly manipulate the internal structure of PostgreSQL databases on a PostgreSQL server. These client programs can be located on the same machine with the PostgreSQL server, or may be on a remote machine which accesses a PostgreSQL server over a network connection. This package contains the docs in HTML for

the whole package, as well as command-line utilities for managing PostgreSQL databases on a PostgreSQL server. If you want to manipulate a PostgreSQL database on a remote PostgreSQL server, you need this package. You also need to install this package if you're installing the postgresql-server package.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

postgresql84-8.4.7-1.el5_6.1 - postgresql84-8.4.9-1.el5_7.1

- Group: Applications/Databases
- Summary: PostgreSQL client programs
- Description: PostgreSQL is an advanced Object-Relational database management system (DBMS) that supports almost all SQL constructs (including transactions, subselects and user-defined types and functions). The postgresql package includes the client programs and libraries that you'll need to access a PostgreSQL DBMS server. These PostgreSQL client programs are programs that directly manipulate the internal structure of PostgreSQL databases on a PostgreSQL server. These client programs can be located on the same machine with the PostgreSQL server, or may be on a remote machine which accesses a PostgreSQL server over a network connection. This package contains the docs in HTML for the whole package, as well as command-line utilities for managing PostgreSQL databases on a PostgreSQL server. If you want to manipulate a PostgreSQL database on a local or remote PostgreSQL server, you need this package. You also need to install this package if you're installing the postgresql-server package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ppc64-utils-0.13-7.el5 - ppc64-utils-0.13-13.el5

- Group: System Environment/Base
- Summary: Linux/PPC64 specific utilities
- Description: A collection of utilities for Linux on PPC64 platforms.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

procinfo-18-19 - procinfo-18-19.el5_7.2

- Group: Applications/System
- Summary: A tool for gathering and displaying system information.
- Description: The procinfo command gets system data from the /proc directory (the kernel filesystem), formats it and displays it on standard output. You can use procinfo to acquire information about your system from the kernel as it is running. Install procinfo if you'd like to use it to gather and display system data.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

procps-3.2.7-17.el5 - procps-3.2.7-18.el5

- Group: Applications/System
- Summary: System and process monitoring utilities.
- Description: The procps package contains a set of system utilities that provide system information. Procps includes ps, free, skill, pkill, pgrep, snice, tload, top, uptime, vmstat, w, watch and pdwx. The ps command displays a snapshot of running processes. The top command provides a repetitive update of the statuses of running processes. The free command displays the amounts of free and used memory on your system. The skill command sends a terminate command (or another specified signal) to a specified set of processes. The snice command is used to change the scheduling priority of specified processes. The tload command prints a graph of the current system load average to a specified tty. The uptime command displays the current time, how long the system has been running, how many users are logged on, and system load averages for the past one, five, and fifteen minutes. The w command displays a list of the users who are currently logged on and what they are running. The watch program watches a running program. The vmstat command displays virtual memory statistics about processes, memory, paging, block I/O, traps, and CPU activity. The pwdx command reports the current working directory of a process or processes.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

python-2.4.3-44.el5 - python-2.4.3-46.el5

- Group: Development/Languages
- Summary: An interpreted, interactive, object-oriented programming language.
- Description: Python is an interpreted, interactive, object-oriented programming language often compared to Tcl, Perl, Scheme or Java. Python includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems (X11, Motif, Tk, Mac and MFC). Programmers can write new built-in modules for Python in C or C++. Python can be used as an extension language for applications that need a programmable interface. This package contains most of the standard Python modules, as well as modules for interfacing to the Tix widget set for Tk and RPM. Note that documentation for Python is provided in the python-docs package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

python-rhsm-0.95.5.5-1.el5 - python-rhsm-0.98.9-1.el5

- Group: Development/Libraries
- Summary: A Python library to communicate with a Red Hat Unified Entitlement Platform
- Description: A small library for communicating with the REST interface of a Red Hat Unified Entitlement Platform. This interface is used for the management of system entitlements, certificates, and access to content.
- Added Dependencies:
  - rpm-python
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

python-virtinst-0.400.3-12.el5 - python-virtinst-0.400.3-13.el5

- Group: Development/Libraries
- Summary: Python modules and utilities for installing virtual machines
- Description: virtinst is a module that helps build and install libvirt based virtual machines. Currently supports KVM, QEmu and Xen virtual machines. Package includes several

command line utilities, including virt-install (build and install new VMs) and virt-clone (clone an existing virtual machine).

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pyxf86config-0.3.31-2.fc6 - pyxf86config-0.3.31-3.el5

- Group: System Environment/Libraries
- Summary: Python wrappers for libxf86config
- Description: Python wrappers for the X server config file library libxf86config. It is used to read and write X server configuration files.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

qt-3.3.6-23.el5 - qt-3.3.6-25.el5

- Group: System Environment/Libraries
- Summary: The shared library for the Qt GUI toolkit.
- Description: Qt is a GUI software toolkit which simplifies the task of writing and maintaining GUI (Graphical User Interface) applications for the X Window System. Qt is written in C++ and is fully object-oriented. This package contains the shared library needed to run qt applications, as well as the README files for qt.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

qt4-4.2.1-1 - qt4-4.2.1-1.el5_7.1

- Group: System Environment/Libraries

- Summary: The shared library for the Qt GUI toolkit
- Description: Qt is a GUI software toolkit which simplifies the task of writing and maintaining GUI (Graphical User Interface) applications for the X Window System. Qt is written in C++ and is fully object-oriented. This package contains the shared library needed to run qt applications, as well as the README files for qt.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rdesktop-1.6.0-3.el5_6.2 - rdesktop-1.6.0-7

- Group: User Interface/Desktops
- Summary: X client for remote desktop into Windows Terminal Server
- Description: rdesktop is an open source client for Windows NT Terminal Server and Windows 2000 & 2003 Terminal Services, capable of natively speaking Remote Desktop Protocol (RDP) in order to present the user's NT desktop. Unlike Citrix ICA, no server extensions are required.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

redhat-release-5Server-5.7.0.3 - redhat-release-5Server-5.8.0.3

- Group: System Environment/Base
- Summary: Red Hat Enterprise Linux release file
- Description: Red Hat Enterprise Linux release files
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

redhat-release-notes-5Server-41 - redhat-release-notes-5Server-43

- Group: System Environment/Base
- Summary: Red Hat Enterprise Linux release notes files
- Description: Red Hat Enterprise Linux release notes files.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rgmanager-2.0.52-21.el5 - rgmanager-2.0.52-28.el5

- Group: System Environment/Base
- Summary: Open Source HA Resource Group Failover for Red Hat Enterprise Linux
- Description: Red Hat Resource Group Manager provides high availability of critical server applications in the event of planned or unplanned system downtime.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhn-client-tools-0.4.20-56.el5 - rhn-client-tools-0.4.20-77.el5

- Group: System Environment/Base
- Summary: Support programs and libraries for Red Hat Network
- Description: Red Hat Network Client Tools provides programs and libraries to allow your system to receive software updates from Red Hat Network.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhnlib-2.5.22-6.el5 - rhnlib-2.5.22-7.el5

- Group: Development/Libraries

- Summary: Python libraries for the RHN project
- Description: rhnlib is a collection of python modules used by the Red Hat Network (http://rhn.redhat.com) software.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhpl-0.194.1-1 - rhpl-0.194.1-2

- Group: System Environment/Libraries
- Summary: Library of python code used by programs in Red Hat Linux
- Description: The rhpl package contains Python code used by programs in Red Hat Linux.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhpxl-0.41.1-9.el5 - rhpxl-0.41.1-12.el5

- Group: System Environment/Libraries
- Summary: Python library for configuring and running X.
- Description: The rhpxl (pronounced 'rapunzel') package contains a Python library for configuring and running X.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rng-utils-2.0-4.el5 - rng-utils-2.0-5.el5

- Group: System Environment/Base
- Summary: Random number generator related utilities
- Description: Hardware random number generation tools.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rpm-4.4.2.3-22.el5 - rpm-4.4.2.3-27.el5

- Group: System Environment/Base
- Summary: The RPM package management system
- Description: The RPM Package Manager (RPM) is a powerful command line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages. Each software package consists of an archive of files along with information about the package like its version, a description, etc.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rsh-0.17-40.el5 - rsh-0.17-40.el5_7.1

- Group: Applications/Internet
- Summary: Clients for remote access commands (rsh, rlogin, rcp).
- Description: The rsh package contains a set of programs which allow users to run commands on remote machines, login to other machines and copy files between machines (rsh, rlogin and rcp). All three of these commands use rhosts style authentication. This package contains the clients needed for all of these services. The rsh package should be installed to enable remote access to other machines.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rsync-3.0.6-4.el5 - rsync-3.0.6-4.el5_7.1

- Group: Applications/Internet
- Summary: A program for synchronizing files over a network
- Description: Rsync uses a reliable algorithm to bring remote and host files into sync very quickly. Rsync is fast because it just sends the differences in the files over the network instead of sending the complete files. Rsync is often used as a very powerful mirroring process or just as a more capable replacement for the rcp command. A technical report which describes the rsync algorithm is included in this package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rsyslog-3.22.1-3.el5_6.1 - rsyslog-3.22.1-7.el5

- Group: System Environment/Daemons
- Summary: Enhanced system logging and kernel message trapping daemon
- Description: Rsyslog is an enhanced, multi-threaded syslog daemon. It supports MySQL, syslog/TCP, RFC 3195, permitted sender lists, filtering on any message part, and fine grain output format control. It is compatible with stock sysklogd and can be used as a drop-in replacement. Rsyslog is simple to set up, with advanced features suitable for enterprise-class, encryption-protected syslog relay chains.
- Added Dependencies:
  - net-snmp-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ruby-1.8.5-19.el5_6.1 - ruby-1.8.5-24.el5

- Group: Development/Languages
- Summary: An interpreter of object-oriented scripting language
- Description: Ruby is the interpreted scripting language for quick and easy object-oriented programming. It has many features to process text files and to do system management tasks (as in Perl). It is simple, straight-forward, and extensible.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

s390utils-1.8.1-16.el5 - s390utils-1.8.1-17.el5

- Group: System Environment/Base
- Summary: Linux/390 specific utilities
- Description: This package contains utilities related to Linux for S/390. The most important programs contained in this package are: - The cmstools suite to list, check, copy and cat files from a CMS volume. - chccwdev, a script to generically change attributes of a ccw device. - dasdfmt, which is used to low-level format eckd-dasds with either the classic linux disk layout or the new z/OS compatible disk layout. - dasdview, which displays DASD and VTOC information and dumps the content of a DASD to the console. - fdasd, which is used to create or modify partitions on eckd-dasds formatted with the z/OS compatible disk layout. - osasnmpd, a subagent for net-snmp to access the OSA hardware. - qetharp to query and purge address data in the OSA and HiperSockets hardware - qethconf to configure IBM QETH function IPA, VIPA and Proxy ARP. - src_vipa.sh to start applications using VIPA capabilities - tunedasd, a tool to adjust tunable parameters on DASD devices - vmconvert, a tool to convert vm dumps to lkcd compatible dumps. - vmcp, a tool to send CP commands from a Linux guest to the VM. - vmur, a tool to work with z/VM spool file queues (reader, punch, printer). - zipl, which is used to make either dasds or tapes bootable for system IPL or system dump. - zdump, which is used to retrieve system dumps from either tapes or dasds. - ziomon tools to collect data for zfcp performance analysis and report. - iucvterm, a z/VM IUCV terminal applications. - cpuplugd, a daemon that manages CPU and memory resources based on a set of rules. - dumpconf, the dump device used for system dump in case a kernel panic occurs. - mon_statd, pair of Linux - z/VM monitoring daemons. - ipl_tools, tool set to configure and list reipl and shutdown actions. - cpi, a service to set the system and sysplex names from the Linux guest to the HMC/SE using the Control Program Identification feature.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sabayon-2.12.4-7.el5 - sabayon-2.12.4-9.el5

- Group: Applications/System
- Summary: Tool to maintain user profiles in a GNOME desktop
- Description: Sabayon is a tool to help sysadmins and user change and maintain the default behaviour of the GNOME desktop. This package contains the graphical tools which a sysadmin use to manage Sabayon profiles.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

samba-3.0.33-3.29.el5_6.2 - samba-3.0.33-3.37.el5

- Group: System Environment/Daemons
- Summary: The Samba SMB server.
- Description: Samba is the suite of programs by which a lot of PC-related machines share files, printers, and other information (such as lists of available files and printers). The Windows NT, OS/2, and Linux operating systems support this natively, and add-on packages can enable the same thing for DOS, Windows, VMS, UNIX of all kinds, MVS, and more. This package provides an SMB server that can be used to provide network services to SMB (sometimes called "Lan Manager") clients. Samba uses NetBIOS over TCP/IP (NetBT) protocols and does NOT need the NetBEUI (Microsoft Raw NetBIOS frame) protocol.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

samba3x-3.5.4-0.83.el5 - samba3x-3.5.10-0.107.el5

- Group: System Environment/Daemons
- Summary: Server and Client software to interoperate with Windows machines
- Description: Samba is the suite of programs by which a lot of PC-related machines share files, printers, and other information (such as lists of available files and printers). The Windows NT, OS/2, and Linux operating systems support this natively, and add-on packages can enable the same thing for DOS, Windows, VMS, UNIX of all kinds, MVS, and more. This package provides an SMB/CIFS server that can be used to provide network services to SMB/CIFS clients. Samba uses NetBIOS over TCP/IP (NetBT) protocols and does NOT need the NetBEUI (Microsoft Raw NetBIOS frame) protocol.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sblim-1-47.el5 - sblim-1-49.el5

- Group: Applications/System
- Summary: Standards Based Linux Instrumentation for Manageability
- Description: SBLIM stands for Standards Based Linux Instrumentation for Manageability, and consists of a set of standards based Web Based Enterprise Management (WBEM) modules that use the Common Information Model (CIM) standard to gather and provide systems management information, events, and methods to local or networked consumers via an CIM object services broker using the CMPI (Common Manageability Programming Interface) standard. This package provides a set of core providers and development tools for systems management applications.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

scim-bridge-0.4.5-9.el5 - scim-bridge-0.4.5-10.el5

- Group: System Environment/Libraries
- Summary: SCIM Bridge Gtk IM module
- Description: SCIM Bridge is a C implementation of a Gtk IM module for SCIM.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

scsi-target-utils-1.0.14-1.el5 - scsi-target-utils-1.0.14-2.el5

- Group: System Environment/Daemons
- Summary: The SCSI target daemon and utility programs
- Description: The SCSI target package contains the daemon and tools to setup a SCSI targets. Currently, software iSCSI targets are supported.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

selinux-policy-2.4.6-316.el5 - selinux-policy-2.4.6-327.el5

- Group: System Environment/Base
- Summary: SELinux policy configuration
- Description: SELinux Reference Policy - modular.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sendmail-8.13.8-8.el5 - sendmail-8.13.8-8.1.el5_7

- Group: System Environment/Daemons
- Summary: A widely used Mail Transport Agent (MTA).
- Description: The Sendmail program is a very widely used Mail Transport Agent (MTA). MTAs send mail from one machine to another. Sendmail is not a client program, which you use to read your email. Sendmail is a behind-the-scenes program which actually moves your email over networks or the Internet to where you want it to go. If you ever need to reconfigure Sendmail, you will also need to have the sendmail.cf package installed. If you need documentation on Sendmail, you can install the sendmail-doc package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

setup-2.5.58-7.el5 - setup-2.5.58-9.el5

- Group: System Environment/Base
- Summary: A set of system configuration and setup files.
- Description: The setup package contains a set of important system configuration and setup files, such as passwd, group, and profile.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

shadow-utils-4.0.17-18.el5_6.1 - shadow-utils-4.0.17-20.el5

- Group: System Environment/Base
- Summary: Utilities for managing accounts and shadow password files.
- Description: The shadow-utils package includes the necessary programs for converting UNIX password files to the shadow password format, plus programs for managing user and group accounts. The pwconv command converts passwords to the shadow password format. The pwunconv command unconverts shadow passwords and generates an npasswd file (a standard UNIX password file). The pwck command checks the integrity of password and shadow files. The lastlog command prints out the last login times for all users. The useradd, userdel, and usermod commands are used for managing user accounts. The groupadd, groupdel, and groupmod commands are used for managing group accounts.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

smartmontools-5.38-2.el5 - smartmontools-5.38-3.el5

- Group: System Environment/Base
- Summary: Tools for monitoring SMART capable hard disks
- Description: The smartmontools package contains two utility programs (smartctl and smartd) to control and monitor storage systems using the Self- Monitoring, Analysis and Reporting Technology System (SMART) built into most modern ATA and SCSI hard disks. In many cases, these utilities will provide advanced warning of disk degradation and failure.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sos-1.7-9.54.el5 - sos-1.7-9.62.el5

- Group: Development/Libraries
- Summary: A set of tools to gather troubleshooting information from a system

- Description: Sos is a set of tools that gathers information about system hardware and configuration. The information can then be used for diagnostic purposes and debugging. Sos is commonly used to help support technicians and developers.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sssd-1.5.1-37.el5 - sssd-1.5.1-49.el5

- Group: Applications/System
- Summary: System Security Services Daemon
- Description: Provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides an NSS and PAM interface toward the system and a pluggable backend system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects like FreeIPA.
- Added Dependencies:
  - diffstat
  - findutils
  - glib2-devel
  - pkgconfig
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

subscription-manager-0.95.5.21-1.el5 - subscription-manager-0.98.14-1.el5

- Group: System Environment/Base
- Summary: Tools and libraries for subscription and repository management
- Description: The Subscription Manager package provides programs and libraries to allow users to manage subscriptions and yum repositories from the Red Hat entitlement platform.
- Added Dependencies:
  - scrollkeeper
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

sudo-1.7.2p1-10.el5 - sudo-1.7.2p1-13.el5

- Group: Applications/System
- Summary: Allows restricted root access for specified users.
- Description: Sudo (superuser do) allows a system administrator to give certain users (or groups of users) the ability to run some (or all) commands as root while logging all commands and arguments. Sudo operates on a per-command basis. It is not a replacement for the shell. Features include: the ability to restrict what commands a user may run on a per-host basis, copious logging of each command (providing a clear audit trail of who did what), a configurable timeout of the sudo command, and the ability to use the same configuration file (sudoers) on many different machines.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

switchdesk-4.0.8-6 - switchdesk-4.0.8-7.el5

- Group: User Interface/Desktops
- Summary: A desktop environment switcher for GNOME, KDE and AnotherLevel.
- Description: The Desktop Switcher is a tool which enables users to easily switch between various desktop environments that they have installed. The tool includes support for KDE, GNOME, XFce4 and twm. Support for different environments on different computers is available, as well as support for setting a global default environment. Install switchdesk if you need a tool for switching between desktop environments.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

syslinux-3.11-4 - syslinux-3.11-7

- Group: Applications/System
- Summary: Simple kernel loader which boots from a FAT filesystem
- Description: SYSLINUX is a suite of bootloaders, currently supporting DOS FAT filesystems, Linux ext2/ext3 filesystems (EXTLINUX), PXE network boots (PXELINUX), or ISO 9660 CD-

ROMs (ISOLINUX). It also includes a tool, MEMDISK, which loads legacy operating systems from these media.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-bind-4.0.3-4.el5 - system-config-bind-4.0.3-5.el5

- Group: Applications/System
- Summary: The Red Hat BIND DNS Configuration Tool.
- Description: The system-config-bind package provides a graphical user interface (GUI) to configure the Berkeley Internet Name Domain (BIND) Domain Name System (DNS) server, "named", with a set of python modules. Users new to BIND configuration can use this tool to quickly set up a working DNS server.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-cluster-1.0.57-9 - system-config-cluster-1.0.57-12

- Group: Applications/System
- Summary: system-config-cluster is a utility which allows you to manage cluster configuration in a graphical setting.
- Description: system-config-cluster is a utility which allows you to manage cluster configuuration in a graphical setting.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-date-1.8.12-4.el5 - system-config-date-1.8.12-5.el5

- Group: System Environment/Base
- Summary: A graphical interface for modifying system date and time
- Description: system-config-date is a graphical interface for changing the system date and time, configuring the system time zone, and setting up the NTP daemon to synchronize the time of the system with an NTP time server.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-display-1.0.48-2.el5 - system-config-display-1.0.48-4.el5

- Group: System Environment/Base
- Summary: A graphical interface for configuring the X Window System display
- Description: system-config-display is a graphical application for configuring an X Window System X server display.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-network-1.3.99.19-2.el5 - system-config-network-1.3.99.21-1.el5

- Group: Applications/System
- Summary: The GUI of the NEtwork Adminstration Tool
- Description: This is the GUI of the network configuration tool, supporting Ethernet, Wireless, TokenRing, ADSL, ISDN and PPP.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-nfs-1.3.23-1.el5 - system-config-nfs-1.3.23-2.el5

- Group: System Environment/Base
- Summary: NFS server configuration tool
- Description: system-config-nfs is a graphical user interface for creating, modifying, and deleting nfs shares.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-printer-0.7.32.10-1.el5 - system-config-printer-0.7.32.10-1.el5_7.1

- Group: System Environment/Base
- Summary: A printer administration tool
- Description: system-config-printer is a graphical user interface that allows the user to configure a CUPS print server.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-users-1.2.51-4.el5 - system-config-users-1.2.51-7.el5

- Group: Applications/System
- Summary: A graphical interface for administering users and groups
- Description: system-config-users is a graphical utility for administrating users and groups. It depends on the libuser library.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-switch-mail-0.5.25-12 - system-switch-mail-0.5.25-13.el5

- Group: Applications/System

- Summary: The Mail Transport Agent Switcher
- Description: The system-switch-mail is the Mail Transport Agent Switcher. It enables users to easily switch between various Mail Transport Agent that they have installed.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

systemtap-1.3-8.el5 - systemtap-1.6-6.el5

- Group: Development/System
- Summary: Instrumentation System
- Description: SystemTap is an instrumentation system for systems running Linux. Developers can write instrumentation to collect data on the operation of the system.
- Added Dependencies:
  - gettext
  - gettext-devel
- Removed Dependencies:
  - nss-tools
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tar-1.15.1-30.el5 - tar-1.15.1-31.el5

- Group: Applications/Archiving
- Summary: A GNU file archiving program
- Description: The GNU tar program saves many files together in one archive and can restore individual files (or all of the files) from that archive. Tar can also be used to add supplemental files to an archive and to update or list files in the archive. Tar includes multivolume support, automatic archive compression/decompression, the ability to perform remote archives, and the ability to perform incremental and full backups. If you want to use tar for remote backups, you also need to install the rmt package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

tog-pegasus-2.9.1-2.el5_5.1 - tog-pegasus-2.11.0-3.el5

- Group: Systems Management/Base
- Summary: OpenPegasus WBEM Services for Linux
- Description: OpenPegasus WBEM Services for Linux enables management solutions that deliver increased control of enterprise resources. WBEM is a platform and resource independent DMTF standard that defines a common information model and communication protocol for monitoring and controlling resources from diverse sources.
- Added Dependencies:
  - rpm
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tomcat5-5.5.23-0jpp.19.el5_6 - tomcat5-5.5.23-0jpp.22.el5_7

- Group: Networking/Daemons
- Summary: Apache Servlet/JSP Engine, RI for Servlet 2.4/JSP 2.0 API
- Description: Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies. The Java Servlet and JavaServer Pages specifications are developed by Sun under the Java Community Process. Tomcat is developed in an open and participatory environment and released under the Apache Software License. Tomcat is intended to be a collaboration of the best-of-breed developers from around the world. We invite you to participate in this open development project. To learn more about getting involved, click here.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tzdata-2011g-1.el5 - tzdata-2011l-4.el5

- Group: System Environment/Base
- Summary: Timezone data
- Description: This package contains data files with rules for various time zones around the world.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

udev-095-14.27.el5 - udev-095-14.27.el5_7.1

- Group: System Environment/Base
- Summary: A userspace implementation of devfs
- Description: The udev package contains an implementation of devfs in userspace using sysfs and netlink.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

unixODBC-2.2.11-7.1 - unixODBC-2.2.11-10.el5

- Group: System Environment/Libraries
- Summary: A complete ODBC driver manager for Linux
- Description: Install unixODBC if you want to access databases through ODBC. This package includes low-level drivers for MySQL, PostgreSQL, and local files. However, the included drivers are not as up-to-date as the ones distributed separately. It is recommended that you install and use the MyODBC package if you need a driver for MySQL, and/or the postgresql-odbc package for PostgreSQL.
- Added Dependencies:
  - libtool >= 1.5.22-7
- Removed Dependencies:
  - libtool
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

util-linux-2.13-0.56.el5 - util-linux-2.13-0.59.el5

- Group: System Environment/Base
- Summary: A collection of basic system utilities.
- Description: The util-linux package contains a large variety of low-level system utilities that are necessary for a Linux system to function. Among others, Util-linux contains the fdisk configuration tool and the login program.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

virt-manager-0.6.1-14.el5 - virt-manager-0.6.1-16.el5

- Group: Applications/Emulators
- Summary: Virtual Machine Manager
- Description: Virtual Machine Manager provides a graphical tool for administering virtual machines for KVM, Xen, and QEmu. Start, stop, add or remove virtual devices, connect to a graphical or serial console, and see resource usage statistics for existing VMs on local or remote machines. Uses libvirt as the backend management API.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

vixie-cron-4.1-77.el5_4.1 - vixie-cron-4.1-81.el5

- Group: System Environment/Base
- Summary: The Vixie cron daemon for executing specified programs at set times.
- Description: The vixie-cron package contains the Vixie version of cron. Cron is a standard UNIX daemon that runs specified programs at scheduled times. Vixie cron adds better security and more powerful configuration options to the standard version of cron.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

vsftpd-2.0.5-21.el5 - vsftpd-2.0.5-24.el5

- Group: System Environment/Daemons
- Summary: vsftpd - Very Secure Ftp Daemon
- Description: vsftpd is a Very Secure FTP daemon. It was written completely from scratch.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xen-3.0.3-132.el5 - xen-3.0.3-135.el5

- Group: Development/Libraries
- Summary: Xen is a virtual machine monitor
- Description: This package contains the Xen tools and management daemons needed to run virtual machines on x86, x86_64, and ia64 systems. Information on how to use Xen can be found at the Xen project pages. The Xen system also requires the Xen hypervisor and domain-0 kernel, which can be found in the kernel-xen* package. Virtualization can be used to run multiple operating systems on one physical system, for purposes of hardware consolidation, hardware abstraction, or to test untrusted applications in a sandboxed environment.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xinetd-2.3.14-13.el5 - xinetd-2.3.14-16.el5

- Group: System Environment/Daemons
- Summary: A secure replacement for inetd.
- Description: Xinetd is a secure replacement for inetd, the Internet services daemon. Xinetd provides access control for all services based on the address of the remote host and/or on time of access and can prevent denial-of-access attacks. Xinetd provides extensive logging, has no limit on the number of server arguments, and lets you bind specific services to specific IP addresses on your host machine. Each service has its own specific configuration file for Xinetd; the files are located in the /etc/xinetd.d directory.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xkeyboard-config-0.8-9.el5 - xkeyboard-config-0.8-10.el5

- Group: User Interface/X
- Summary: xkeyboard-config alternative xkb data files
- Description: xkeyboard-config alternative xkb data files
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xmlrpc-c-1.16.24-1206.1840.el5 - xmlrpc-c-1.16.24-1206.1840.4.el5

- Group: System Environment/Libraries
- Summary: A lightweight RPC library based on XML and HTTP
- Description: XML-RPC is a quick-and-easy way to make procedure calls over the Internet. It converts the procedure call into XML document, sends it to a remote server using HTTP, and gets back the response as XML. This library provides a modular implementation of XML-RPC for C.
- Added Dependencies:
  - curl-devel >= 7.15.5-15
- Removed Dependencies:
  - curl-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-drv-i810-1.6.5-9.36.el5 - xorg-x11-drv-i810-1.6.5-9.40.el5

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 i810 video driver(s)
- Description: X.Org X11 i810 video driver.
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-drv-mga-1.4.13-2.el5 - xorg-x11-drv-mga-1.4.13-5.el5

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 mga video driver
- Description: X.Org X11 mga video driver.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-drv-sis-0.9.1-7.3.el5 - xorg-x11-drv-sis-0.9.1-7.3.el5_7.1

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 sis video driver
- Description: X.Org X11 sis video driver.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-server-1.1.1-48.76.el5_6.4 - xorg-x11-server-1.1.1-48.90.el5

- Group: User Interface/X
- Summary: X.Org X11 X server
- Description: X.Org X11 X server
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xulrunner-1.9.2.18-2.el5_6 - xulrunner-1.9.2.26-1.el5_7

- Group: Applications/Internet
- Summary: XUL Runtime for Gecko Applications
- Description: XULRunner provides the XUL Runtime environment for Gecko applications.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yaboot-1.3.13-12.el5 - yaboot-1.3.13-14.el5

- Group: System Environment/Base
- Summary: Linux bootloader for Power Macintosh "New World" computers.
- Description: yaboot is a bootloader for PowerPC machines which works on New World ROM machines (Rev. A iMac and newer) and runs directly from Open Firmware, eliminating the need for Mac OS. yaboot can also bootload IBM pSeries machines.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yp-tools-2.9-1.el5 - yp-tools-2.9-2.el5

- Group: System Environment/Base
- Summary: NIS (or YP) client programs.
- Description: The Network Information Service (NIS) is a system which provides network information (login names, passwords, home directories, group information) to all of the machines on a network. NIS can enable users to login on any machine on the network, as long as the machine has the NIS client programs running and the user's password is recorded in the NIS passwd database. NIS was formerly known as Sun Yellow Pages (YP). This package's NIS implementation is based on FreeBSD's YP and is a special port for glibc 2.x and libc versions 5.4.21 and later. This package only provides the NIS client programs. In order to use the clients, you'll need to already have an NIS server running on your network.

An NIS server is provided in the ypserv package. Install the yp-tools package if you need NIS client programs for machines on your network. You will also need to install the ypbind package on every machine running NIS client programs. If you need an NIS server, you'll need to install the ypserv package on one machine on the network.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ypserv-2.19-5.el5_6.1 - ypserv-2.19-9.el5

- Group: System Environment/Daemons
- Summary: The NIS (Network Information Service) server.
- Description: The Network Information Service (NIS) is a system that provides network information (login names, passwords, home directories, group information) to all of the machines on a network. NIS can allow users to log in on any machine on the network, as long as the machine has the NIS client programs running and the user's password is recorded in the NIS passwd database. NIS was formerly known as Sun Yellow Pages (YP). This package provides the NIS server, which will need to be running on your network. NIS clients do not need to be running the server. Install ypserv if you need an NIS server for your network. You also need to install the yp-tools and ypbind packages on any NIS client machines.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yum-3.2.22-37.el5 - yum-3.2.22-39.el5

- Group: System Environment/Base
- Summary: RPM installer/updater
- Description: Yum is a utility that can check for and automatically download and install updated RPM packages. Dependencies are obtained and downloaded automatically prompting the user as necessary.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

yum-rhn-plugin-0.5.4-22.el5 - yum-rhn-plugin-0.5.4-26.el5

- Group: System Environment/Base
- Summary: RHN support for yum
- Description: This yum plugin provides support for yum to access a Red Hat Network server for software updates.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yum-utils-1.1.16-16.el5 - yum-utils-1.1.16-21.el5

- Group: Development/Tools
- Summary: Utilities based around the yum package manager
- Description: yum-utils is a collection of utilities and examples for the yum package manager. It includes utilities by different authors that make yum easier and more powerful to use. These tools include: debuginfo-install, package-cleanup, repoclosure, repodiff, repo-graph, repomanage, repoquery, repo-rss, reposync, repotrack, verifytree, yum-builddep, yum-complete-transaction, yumdownloader, yum-debug-dump and yum-groups-manager.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

zsh-4.2.6-5.el5 - zsh-4.2.6-6.el5

- Group: System Environment/Shells
- Summary: A powerful interactive shell
- Description: The zsh shell is a command interpreter usable as an interactive login shell and as a shell script command processor. Zsh resembles the ksh shell (the Korn shell), but includes many enhancements. Zsh supports command line editing, built-in spelling correction, programmable command completion, shell functions (with autoloading), a history mechanism, and more.
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

A.2. Client

A.2.1. Added Packages

binutils220-2.20.51.0.2-5.29.el5

- Group: Development/Tools
- Summary: Binary utilities for the preview of GCC version 4.4
- Description: The binutils220 package contains the assembler and objdump utility for the preview of GCC version 4.4.

iotop-0.4.3-4.el5

- Group: Applications/System
- Summary: Top like utility for I/O
- Description: Linux has always been able to show how much I/O was going on (the bi and bo columns of the vmstat 1 command). iotop is a Python program with a top like UI used to show of behalf of which process is the I/O going on.

mysql-connector-odbc64-5.1.8-1.el5

- Group: System Environment/Libraries
- Summary: ODBC driver for MySQL
- Description: An ODBC (rev 3) driver for MySQL, for use with unixODBC64.

pixman-0.22.0-2.el5

- Group: System Environment/Libraries
- Summary: Pixel manipulation library
- Description: Pixman is a pixel manipulation library for X and cairo.

postgresql-odbc64-09.00.0200-1.el5

- Group: Applications/Databases
- Summary: PostgreSQL ODBC driver
- Description: This package includes the driver needed for applications to access a PostgreSQL system via ODBC (Open Database Connectivity). This version is for use with unixODBC64.

python-ctypes-1.0.2-3.el5

- Group: Development/Libraries
- Summary: Create and manipulate C data types from Python
- Description: python-ctypes is a python module to create and manipulate C data types in Python, and to call functions in dynamic link libraries/shared dlls. It allows wrapping these libraries in pure Python.

spice-client-0.8.1-6.el5

- Group: User Interface/Desktops
- Summary: Implements the client side of the SPICE protocol
- Description: The Simple Protocol for Independent Computing Environments (SPICE) is a remote display system built for virtual environments which allows you to view a computing 'desktop' environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures. This package contains the SPICE client application.

spice-protocol-0.8.0-2.el5

- Group: Development/Libraries
- Summary: Spice protocol header files
- Description: Header files describing the spice protocol and the para-virtual graphics card QXL.

subscription-manager-migration-data-1.11-1.el5

- Group: System Environment/Base
- Summary: RHN Classic to RHSM migration data
- Description: This package provides certificates for migrating a system from RHN Classic to RHSM.

unixODBC64-2.2.14-3.el5

- Group: System Environment/Libraries
- Summary: A complete ODBC driver manager for Linux
- Description: Install unixODBC64 if you want to access databases through ODBC, and you need to use the corrected 64-bit ABI used in unixODBC 2.2.12 and up. This base package provides documentation and command-line utility programs, but is not required for client applications to make use of unixODBC64. You will also need the mysql-connector-odbc64 package if you want to access a MySQL database, and/or the postgresql-odbc64 package for PostgreSQL.

virt-who-0.5-5.el5

- Group: System Environment/Base
- Summary: Agent for reporting virtual guest IDs to subscription-manager
- Description: Agent that collects information about virtual guests present in the system and report them to the subscription manager.

A.2.2. Dropped Packages

qspice-client-0.3.0-4.el5_5

- Group: User Interface/Desktops
- Summary: Implements the client side of the SPICE protocol
- Description: The Simple Protocol for Independent Computing Environments (SPICE) is a remote display system built for virtual environments which allows you to view a computing 'desktop' environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures. This package provides the client side of the SPICE protocol

A.2.3. Updated Packages

Deployment_Guide-5.2-11 - Deployment_Guide-5.8-1.el5

- Group: Documentation
- Summary: Deployment Guide
- Description: This Deployment Guide documents relevant information regarding the deployment, configuration and administration of Red Hat Enterprise Linux 5.8.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ImageMagick-6.2.8.0-4.el5_5.3 - ImageMagick-6.2.8.0-12.el5

- Group: Applications/Multimedia
- Summary: An X application for displaying and manipulating images.
- Description: ImageMagick(TM) is an image display and manipulation tool for the X Window System. ImageMagick can read and write JPEG, TIFF, PNM, GIF, and Photo CD image formats. It can resize, rotate, sharpen, color reduce, or add special effects to an image, and when finished you can either save the completed work in the original format or a different one. ImageMagick also includes command line programs for creating animated or transparent .gifs, creating composite images, creating thumbnail images, and more. ImageMagick is one of your choices if you need a program to manipulate and dis play images. If you want to develop your own applications which use ImageMagick code or APIs, you need to install ImageMagick-devel as well.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

MySQL-python-1.2.1-1 - MySQL-python-1.2.3-0.1.c1.el5

- Group: Development/Libraries
- Summary: An interface to MySQL
- Description: Python interface to MySQL MySQLdb is an interface to the popular MySQL database server for Python. The design goals are: - Compliance with Python database API version 2.0 - Thread-safety - Thread-friendliness (threads will not block each other) - Compatibility with MySQL 3.23 and up This module should be mostly compatible with an older interface written by Joe Skinner and others. However, the older version is a) not thread-friendly, b) written for MySQL 3.21, c) apparently not actively maintained. No code from that version is used in MySQLdb.
- Added Dependencies:
  - python-devel
  - python-setuptools
- Removed Dependencies:
  - Distutils
  - gcc
  - python
  - python-devel >= 2.4
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

OpenIPMI-2.0.16-11.el5 - OpenIPMI-2.0.16-12.el5

- Group: System Environment/Base
- Summary: OpenIPMI (Intelligent Platform Management Interface) library and tools
- Description: The Open IPMI project aims to develop an open code base to allow access to platform information using Intelligent Platform Management Interface (IPMI). This package contains the tools of the OpenIPMI project.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

PyXML-0.8.4-4.el5_4.2 - PyXML-0.8.4-6.el5

- Group: Development/Libraries
- Summary: XML libraries for python.
- Description: An XML package for Python. The distribution contains a validating XML parser, an implementation of the SAX and DOM programming interfaces and an interface to the Expat parser.
- Added Dependencies:
  - python-setuptools
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

SDL-1.2.10-8.el5 - SDL-1.2.10-9.el5

- Group: System Environment/Libraries
- Summary: A cross-platform multimedia library.
- Description: Simple DirectMedia Layer (SDL) is a cross-platform multimedia library designed to provide fast access to the graphics frame buffer and audio device.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

Virtualization-5.2-11 - Virtualization-5.8-1.el5

- Group: Documentation
- Summary: Virtualization Guide
- Description: The Red Hat Enterprise Linux Virtualization Guide contains information on installation, configuring, administering, tips, tricks and troubleshooting virtualization technologies used in Red Hat Enterprise Linux.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

acl-2.2.39-6.el5 - acl-2.2.39-8.el5

- Group: System Environment/Base
- Summary: Access control list utilities.
- Description: This package contains the getfacl and setfacl utilities needed for manipulating access control lists.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

acpid-1.0.4-9.el5_4.2 - acpid-1.0.4-12.el5

- Group: System Environment/Daemons
- Summary: ACPI Event Daemon
- Description: acpid is a daemon that dispatches ACPI events to user-space programs.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

alsa-utils-1.0.17-1.el5 - alsa-utils-1.0.17-6.el5

- Group: Applications/Multimedia
- Summary: Advanced Linux Sound Architecture (ALSA) utilities
- Description: This package contains command line utilities for the Advanced Linux Sound Architecture (ALSA).
- Added Dependencies:
  - autoconf
  - automake
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

amanda-2.5.0p2-8.el5 - amanda-2.5.0p2-9.el5

- Group: Applications/System
- Summary: A network-capable tape backup solution.
- Description: AMANDA, the Advanced Maryland Automatic Network Disk Archiver, is a backup system that allows the administrator of a LAN to set up a single master backup server to back up multiple hosts to one or more tape drives or disk files. AMANDA uses native dump and/or GNU tar facilities and can back up a large number of workstations running multiple versions of Unix. Newer versions of AMANDA (including this version) can use SAMBA to back up Microsoft(TM) Windows95/NT hosts. The amanda package contains the core AMANDA programs and will need to be installed on both AMANDA clients and AMANDA servers. Note that you will have to install the amanda-client and/or amanda-server packages as well.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

anaconda-11.1.2.242-1 - anaconda-11.1.2.250-1

- Group: Applications/System
- Summary: Graphical system installer
- Description: The anaconda package contains the program which was used to install your system. These files are of little use on an already installed system.
- Added Dependencies:
  - kudzu-devel >= 1.2.57.1.26-3
  - libdhcp-devel >= 1.20-13
- Removed Dependencies:
  - kudzu-devel >= 1.2.57.1.26-1
  - libdhcp-devel >= 1.20-10
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

arptables_jf-0.0.8-8 - arptables_jf-0.0.8-11.el5

- Group: System Environment/Base
- Summary: Userspace control program for the arptables network filter.

- Description: The arptables_jf utility controls the arpfilter network packet filtering code in the Linux kernel. You do not need this program for normal network firewalling. If you need to manually control which arp requests and/or replies this machine accepts and sends, you should install this package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

aspell-0.60.3-7.1 - aspell-0.60.3-12

- Group: Applications/Text
- Summary: A spelling checker.
- Description: GNU Aspell is a spell checker designed to eventually replace Ispell. It can either be used as a library or as an independent spell checker. Its main feature is that it does a much better job of coming up with possible suggestions than just about any other spell checker out there for the English language, including Ispell and Microsoft Word. It also has many other technical enhancements over Ispell such as using shared memory for dictionaries and intelligently handling personal dictionaries when more than one Aspell process is open at once.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

aspell-sr-0.02-1.2.1 - aspell-sr-0.02-2

- Group: Applications/Text
- Summary: Serbian dictionaries for Aspell.
- Description: Provides the word list/dictionaries for the following: Serbian
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

audit-1.7.18-2.el5 - audit-1.8-2.el5

- Group: System Environment/Daemons
- Summary: User space tools for 2.6 kernel auditing
- Description: The audit package contains the user space utilities for storing and searching the audit records generate by the audit subsystem in the Linux 2.6 kernel.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

autofs-5.0.1-0.rc2.156.el5 - autofs-5.0.1-0.rc2.163.el5

- Group: System Environment/Daemons
- Summary: A tool for automatically mounting and unmounting filesystems.
- Description: autofs is a daemon which automatically mounts filesystems when you use them, and unmounts them later when you are not using them. This can include network filesystems, CD-ROMs, floppies, and so forth.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

bind-9.3.6-16.P1.el5 - bind-9.3.6-20.P1.el5

- Group: System Environment/Daemons
- Summary: The Berkeley Internet Name Domain (BIND) DNS (Domain Name System) server.
- Description: BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating properly.
- Added Dependencies:
  - docbook-style-xsl
  - libxslt
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

bind97-9.7.0-6.P2.el5_6.3 - bind97-9.7.0-6.P2.el5_7.4

- Group: System Environment/Daemons
- Summary: The Berkeley Internet Name Domain (BIND) DNS (Domain Name System) server
- Description: BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating properly.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

binutils-2.17.50.0.6-14.el5 - binutils-2.17.50.0.6-20.el5

- Group: Development/Tools
- Summary: A GNU collection of binary utilities.
- Description: Binutils is a collection of binary utilities, including ar (for creating, modifying and extracting from archives), as (a family of GNU assemblers), gprof (for displaying call graph profile data), ld (the GNU linker), nm (for listing symbols from object files), objcopy (for copying and translating object files), objdump (for displaying information from object files), ranlib (for generating an index for the contents of an archive), size (for listing the section sizes of an object or archive file), strings (for listing printable strings from files), strip (for discarding symbols), and addr2line (for converting addresses to file and line).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

boost-1.33.1-10.el5 - boost-1.33.1-15.el5

- Group: System Environment/Libraries
- Summary: The Boost C++ Libraries
- Description: Boost provides free peer-reviewed portable C++ source libraries. The emphasis is on libraries which work well with the C++ Standard Library, in the hopes of

establishing "existing practice" for extensions and providing reference implementations so that the Boost libraries are suitable for eventual standardization. (Some of the libraries have already been proposed for inclusion in the C++ Standards Committee's upcoming C++ Standard Library Technical Report.)
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

bootparamd-0.17-26.el5 - bootparamd-0.17-26.el5_7.1

- Group: System Environment/Daemons
- Summary: A server process which provides boot information to diskless clients.
- Description: The bootparamd process provides bootparamd, a server process which provides the information needed by diskless clients in order for them to successfully boot. Bootparamd looks first in /etc/bootparams for an entry for that particular client; if a local bootparams file doesn't exist, it looks at the appropriate Network Information Service (NIS) map. Some network boot loaders (notably Sun's) rely on special boot server code on the server, in addition to the RARP and TFTP servers. This bootparamd server process is compatible with SunOS bootparam clients and servers which need that boot server code. You should install bootparamd if you need to provide boot information to diskless clients on your network.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

busybox-1.2.0-10.el5 - busybox-1.2.0-13.el5

- Group: System Environment/Shells
- Summary: Statically linked binary providing simplified versions of system commands
- Description: Busybox is a single binary which includes versions of a large number of system commands, including a shell. This package can be very useful for recovering from certain types of system failures, particularly those involving broken shared libraries.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

cdparanoia-alpha9.8-27.2 - cdparanoia-alpha9.8-28

- Group: Applications/Multimedia
- Summary: A Compact Disc Digital Audio (CDDA) extraction tool (or ripper).
- Description: Cdparanoia (Paranoia III) reads digital audio directly from a CD, then writes the data to a file or pipe in WAV, AIFC or raw 16 bit linear PCM format. Cdparanoia doesn't contain any extra features (like the ones included in the cdda2wav sampling utility). Instead, cdparanoia's strength lies in its ability to handle a variety of hardware, including inexpensive drives prone to misalignment, frame jitter and loss of streaming during atomic reads. Cdparanoia is also good at reading and repairing data from damaged CDs.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

certmonger-0.42-1.el5 - certmonger-0.50-3.el5

- Group: System Environment/Daemons
- Summary: Certificate status monitor and PKI enrollment client
- Description: Certmonger is a service which is primarily concerned with getting your system enrolled with a certificate authority (CA) and keeping it enrolled.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cman-2.0.115-85.el5 - cman-2.0.115-96.el5

- Group: System Environment/Base
- Summary: cman - The Cluster Manager
- Description: cman - The Cluster Manager
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

comps-extras-11.1-1.1 - comps-extras-11.4-1

- Group: Applications/System
- Summary: Images for components included in Fedora
- Description: This package contains images for the components included in Fedora.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

crash-4.1.2-8.el5 - crash-5.1.8-1.el5

- Group: Development/Debuggers
- Summary: Kernel crash and live system analysis utility
- Description: The core analysis suite is a self-contained tool that can be used to investigate either live systems, kernel core dumps created from the netdump, diskdump and kdump packages from Red Hat Linux, the mcore kernel patch offered by Mission Critical Linux, or the LKCD kernel patch.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cups-1.3.7-26.el5_6.1 - cups-1.3.7-30.el5

- Group: System Environment/Daemons
- Summary: Common Unix Printing System
- Description: The Common UNIX Printing System provides a portable printing layer for UNIX® operating systems. It has been developed by Easy Software Products to promote a standard printing solution for all UNIX vendors and users. CUPS provides the System V and Berkeley command-line interfaces.
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

curl-7.15.5-9.el5_6.3 - curl-7.15.5-15.el5

- Group: Applications/Internet
- Summary: A utility for getting files from remote servers (FTP, HTTP, and others).
- Description: cURL is a tool for getting files from FTP, HTTP, Gopher, Telnet, and Dict servers, using any of the supported protocols. cURL is designed to work without user interaction or any kind of interactivity. cURL offers many useful capabilities, like proxy support, user authentication, FTP upload, HTTP post, and file transfer resume.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cvs-1.11.22-7.el5 - cvs-1.11.22-11.el5

- Group: Development/Tools
- Summary: A version control system.
- Description: CVS (Concurrent Versions System) is a version control system that can record the history of your files (usually, but not always, source code). CVS only stores the differences between versions, instead of every version of every file you have ever created. CVS also keeps a log of who, when, and why changes occurred. CVS is very helpful for managing releases and controlling the concurrent editing of source files among multiple authors. Instead of providing version control for a collection of files in a single directory, CVS provides version control for a hierarchical collection of directories consisting of revision controlled files. These directories and files can then be combined together to form a software release.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cyrus-imapd-2.3.7-12.el5 - cyrus-imapd-2.3.7-12.el5_7.2

- Group: System Environment/Daemons
- Summary: A high-performance mail server with IMAP, POP3, NNTP and SIEVE support
- Description: The cyrus-imapd package contains the core of the Cyrus IMAP server. It is a scaleable enterprise mail system designed for use from small to large enterprise environments using standards-based internet mail technologies. A full Cyrus IMAP implementation allows a seamless mail and bulletin board environment to be set up across multiple servers. It differs from other IMAP server implementations in that it is run on "sealed" servers, where users are not normally permitted to log in and have no system account on the server. The mailbox database is stored in parts of the filesystem that are private to the Cyrus IMAP server. All user access to mail is through software using the IMAP, POP3 or KPOP protocols. It also includes support for virtual domains, NNTP, mailbox annotations, and much more. The private mailbox database design gives the server large advantages in efficiency, scalability and administratability. Multiple concurrent read/write connections to the same mailbox are permitted. The server supports access control lists on mailboxes and storage quotas on mailbox hierarchies. The Cyrus IMAP server supports the IMAP4rev1 protocol described in RFC 3501. IMAP4rev1 has been approved as a proposed standard. It supports any authentication mechanism available from the SASL library, imaps/pop3s/nntps (IMAP/POP3/NNTP encrypted using SSL and TLSv1) can be used for security. The server supports single instance store where possible when an email message is addressed to multiple recipients, SIEVE provides server side email filtering.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dapl-2.0.25-2.el5_6.1 - dapl-2.0.25-2.3.el5

- Group: System Environment/Libraries
- Summary: Library providing access to the DAT 1.2 and 2.0 APIs
- Description: libdat and libdapl provide a userspace implementation of the DAT 1.2 and 2.0 API that is built to natively support InfiniBand/iWARP network technology.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dbus-1.1.2-15.el5_6 - dbus-1.1.2-16.el5_7

- Group: System Environment/Libraries
- Summary: D-BUS message bus
- Description: D-BUS is a system for sending messages between applications. It is used both for the systemwide message bus service, and as a per-user-login-session messaging facility.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

device-mapper-1.02.63-4.el5 - device-mapper-1.02.67-2.el5

- Group: System Environment/Base
- Summary: device mapper library
- Description: This package contains the supporting userspace files (libdevmapper and dmsetup) for the device-mapper.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

device-mapper-multipath-0.4.7-46.el5 - device-mapper-multipath-0.4.7-48.el5

- Group: System Environment/Base
- Summary: Tools to manage multipath devices using device-mapper.
- Description: device-mapper-multipath provides tools to manage multipath devices by instructing the device-mapper multipath kernel module what to do. The tools are : * multipath : Scan the system for multipath devices and assemble them. * multipathd : Detects when paths fail and execs multipath to update things.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dhcp-3.0.5-29.el5 - dhcp-3.0.5-31.el5

- Group: System Environment/Daemons
- Summary: DHCP (Dynamic Host Configuration Protocol) server and relay agent.
- Description: DHCP (Dynamic Host Configuration Protocol) is a protocol which allows individual devices on an IP network to get their own network configuration information (IP address, subnetmask, broadcast address, etc.) from a DHCP server. The overall purpose of DHCP is to make it easier to administer a large network. The dhcp package includes the ISC DHCP service and relay agent. To use DHCP on your network, install a DHCP service (or relay agent), and on clients run a DHCP client daemon. The dhcp package provides the ISC DHCP service and relay agent.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dovecot-1.0.7-7.el5 - dovecot-1.0.7-7.el5_7.1

- Group: System Environment/Daemons
- Summary: Dovecot Secure imap server
- Description: Dovecot is an IMAP server for Linux/UNIX-like systems, written with security primarily in mind. It also contains a small POP3 server. It supports mail in either of maildir or mbox formats.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dstat-0.6.6-3.el5_4.1 - dstat-0.6.6-5.el5

- Group: System Environment/Base
- Summary: Versatile resource statistics tool
- Description: Dstat is a versatile replacement for vmstat, iostat, netstat and ifstat. Dstat overcomes some of their limitations and adds some extra features, more counters and flexibility. Dstat is handy for monitoring systems during performance tuning tests, benchmarks or troubleshooting. Dstat allows you to view all of your system resources instantly, you can eg. compare disk usage in combination with interrupts from your IDE controller, or compare the network bandwidth numbers directly with the disk throughput (in the same interval). Dstat gives you detailed selective information in columns and clearly indicates in what magnitude and unit the output is displayed. Less confusion, less mistakes.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dump-0.4b41-5.el5 - dump-0.4b41-6.el5

- Group: Applications/Archiving
- Summary: Programs for backing up and restoring ext2/ext3 filesystems
- Description: The dump package contains both dump and restore. Dump examines files in a filesystem, determines which ones need to be backed up, and copies those files to a specified disk, tape, or other storage medium. The restore command performs the inverse function of dump; it can restore a full backup of a filesystem. Subsequent incremental backups can then be layered on top of the full backup. Single files and directory subtrees may also be restored from full or partial backups. Install dump if you need a system for both backing up filesystems and restoring filesystems after backups.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ecryptfs-utils-75-5.el5 - ecryptfs-utils-75-8.el5

- Group: System Environment/Base
- Summary: The eCryptfs mount helper and support libraries
- Description: eCryptfs is a stacked cryptographic filesystem that ships in the Linux kernel. This package provides the mount helper and supporting libraries to perform key management and mount functions. Install ecryptfs-utils if you would like to mount eCryptfs.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

esound-0.2.36-3 - esound-0.2.36-4

- Group: System Environment/Daemons
- Summary: Allows several audio streams to play on a single audio device.
- Description: EsounD, the Enlightened Sound Daemon, is a server process that mixes several audio streams for playback by a single audio device. For example, if you're listening to music on a CD and you receive a sound-related event from ICQ, the two applications won't have to queue for the use of your sound card. Install esound if you'd like to let sound applications share your audio device. You'll also need to install the audiofile package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

evince-0.6.0-13.el5 - evince-0.6.0-17.el5

- Group: Applications/Publishing
- Summary: Document viewer
- Description: evince is a GNOME-based document viewer.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

expect-5.43.0-5.1 - expect-5.43.0-8.el5

- Group: Development/Languages
- Summary: A program-script interaction and testing utility
- Description: Expect is a tcl application for automating and testing interactive applications such as telnet, ftp, passwd, fsck, rlogin, tip, etc. Expect makes it easy for a script to control another program and interact with it. This package contains expect and some scripts that use it.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

fcoe-utils-1.0.7-4.el5 - fcoe-utils-1.0.7-5.el5

- Group: Applications/System
- Summary: Fibre Channel over Ethernet utilities
- Description: Fibre Channel over Ethernet utilities fcoeadm - command line tool for configuring FCoE interfaces fcoemon - service to configure DCB Ethernet QOS filters, works with dcbd
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

fetchmail-6.3.6-1.1.el5_3.1 - fetchmail-6.3.6-4.el5

- Group: Applications/Internet
- Summary: A remote mail retrieval and forwarding utility
- Description: Fetchmail is a remote mail retrieval and forwarding utility intended for use over on-demand TCP/IP links, like SLIP or PPP connections. Fetchmail supports every remote-mail protocol currently in use on the Internet (POP2, POP3, RPOP, APOP, KPOP, all IMAPs, ESMTP ETRN, IPv6, and IPSEC) for retrieval. Then Fetchmail forwards the mail through SMTP so you can read it through your favorite mail client. Install fetchmail if you need to retrieve mail over SLIP or PPP connections.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

file-4.17-15.el5_3.1 - file-4.17-21

- Group: Applications/File
- Summary: A utility for determining file types.
- Description: The file command is used to identify a particular file according to the type of data contained by the file. File can identify many different file types, including ELF binaries, system libraries, RPM packages, and different graphics formats. You should install the file package, since the file command is such a useful utility.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

firefox-3.6.18-1.el5_6 - firefox-3.6.26-1.el5_7

- Group: Applications/Internet
- Summary: Mozilla Firefox Web browser
- Description: Mozilla Firefox is an open-source web browser, designed for standards compliance, performance and portability.
- Added Dependencies:
  - xulrunner-devel >= 1.9.2.26-1
- Removed Dependencies:
  - xulrunner-devel >= 1.9.2.18-1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

firstboot-1.4.27.8-1.el5 - firstboot-1.4.27.9-1.el5

- Group: System Environment/Base
- Summary: Initial system configuration utility
- Description: The firstboot utility runs after installation. It guides the user through a series of steps that allows for easier configuration of the machine.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

foomatic-3.0.2-38.3.el5 - foomatic-3.0.2-38.3.el5_7.1

- Group: System Environment/Libraries
- Summary: Foomatic printer database.
- Description: Foomatic is a comprehensive, spooler-independent database of printers, printer drivers, and driver descriptions. It contains utilities to generate driver description files and printer queues for CUPS, LPD, LPRng, and PDQ using the database. There is also the possibility to read the PJL options out of PJL-capable laser printers and take them into account at the driver description file generation. There are spooler-independent command

line interfaces to manipulate queues (foomatic-configure) and to print files/manipulate jobs (foomatic printjob). The site http://www.linuxprinting.org/ is based on this database.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

freeradius2-2.1.7-7.el5 - freeradius2-2.1.12-3.el5

- Group: System Environment/Daemons
- Summary: High-performance and highly configurable free RADIUS server
- Description: The FreeRADIUS Server Project is a high performance and highly configurable GPL'd free RADIUS server. The server is similar in some respects to Livingston's 2.0 server. While FreeRADIUS started as a variant of the Cistron RADIUS server, they don't share a lot in common any more. It now has many more features than Cistron or Livingston, and is much more configurable. FreeRADIUS is an Internet authentication daemon, which implements the RADIUS protocol, as defined in RFC 2865 (and others). It allows Network Access Servers (NAS boxes) to perform authentication for dial-up users. There are also RADIUS clients available for Web servers, firewalls, Unix logins, and more. Using RADIUS allows authentication and authorization for a network to be centralized, and minimizes the amount of re-configuration which has to be done when adding or deleting new users.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

freetype-2.2.1-28.el5_5.1 - freetype-2.2.1-28.el5_7.2

- Group: System Environment/Libraries
- Summary: A free and portable font rendering engine
- Description: The FreeType engine is a free and portable font rendering engine, developed to provide advanced font support for a variety of platforms and environments. FreeType is a library which can open and manages font files as well as efficiently load, hint and render individual glyphs. FreeType is not a font server or a complete text-rendering library.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

ftp-0.17-35.el5 - ftp-0.17-37.el5

- Group: Applications/Internet
- Summary: The standard UNIX FTP (File Transfer Protocol) client.
- Description: The ftp package provides the standard UNIX command-line FTP (File Transfer Protocol) client. FTP is a widely used protocol for transferring files over the Internet and for archiving files. If your system is on a network, you should install ftp in order to do file transfers.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gamin-0.1.7-8.el5 - gamin-0.1.7-10.el5

- Group: Development/Libraries
- Summary: Library providing the FAM File Alteration Monitor API
- Description: This C library provides an API and ABI compatible file alteration monitor mechanism compatible with FAM but not dependent on a system wide daemon.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gawk-3.1.5-14.el5 - gawk-3.1.5-15.el5

- Group: Applications/Text
- Summary: The GNU version of the awk text processing utility.
- Description: The gawk packages contains the GNU version of awk, a text processing utility. Awk interprets a special-purpose programming language to do quick and easy text pattern matching and reformatting jobs. Install the gawk package if you need a text processing utility. Gawk is considered to be a standard Linux tool for processing text.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gcc-4.1.2-51.el5 - gcc-4.1.2-52.el5

- Group: Development/Languages
- Summary: Various compilers (C, C++, Objective-C, Java, ...)
- Description: The gcc package contains the GNU Compiler Collection version 4.1. You'll need this package in order to compile C code.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gcc44-4.4.4-13.el5 - gcc44-4.4.6-3.el5.1

- Group: Development/Languages
- Summary: Preview of GCC version 4.4
- Description: The gcc44 package contains preview of the GNU Compiler Collection version 4.4.
- Added Dependencies:
  - binutils220
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gdb-7.0.1-37.el5 - gdb-7.0.1-42.el5

- Group: Development/Debuggers
- Summary: A GNU source-level debugger for C, C++, Java and other languages
- Description: GDB, the GNU debugger, allows you to debug programs written in C, C++, Java, and other languages, by executing them in a controlled fashion and printing their data.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gdbm-1.8.0-26.2.1 - gdbm-1.8.0-26.2.1.el5_6.1

- Group: System Environment/Libraries
- Summary: A GNU set of database routines which use extensible hashing.
- Description: Gdbm is a GNU database indexing library, including routines which use extensible hashing. Gdbm works in a similar way to standard UNIX dbm routines. Gdbm is useful for developers who write C applications and need access to a simple and efficient database or who are building C applications which will use such a database. If you're a C developer and your programs need access to simple database routines, you should install gdbm. You'll also need to install gdbm-devel.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gdm-2.16.0-56.el5 - gdm-2.16.0-59.el5

- Group: User Interface/X
- Summary: The GNOME Display Manager.
- Description: Gdm (the GNOME Display Manager) is a highly configurable reimplementation of xdm, the X Display Manager. Gdm allows you to log into your system with the X Window System running and supports running several different X sessions on your local machine at the same time.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gfs2-utils-0.1.62-31.el5 - gfs2-utils-0.1.62-34.el5

- Group: System Environment/Kernel
- Summary: Utilities for managing the global filesystem (GFS)

- Description: The gfs2-utils package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in GFS filesystems.
- Added Dependencies:
  - zlib-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ghostscript-8.70-6.el5 - ghostscript-8.70-14.el5

- Group: Applications/Publishing
- Summary: A PostScript(TM) interpreter and renderer.
- Description: Ghostscript is a set of software that provides a PostScript(TM) interpreter, a set of C procedures (the Ghostscript library, which implements the graphics capabilities in the PostScript language) and an interpreter for Portable Document Format (PDF) files. Ghostscript translates PostScript code into many common, bitmapped formats, like those understood by your printer or screen. Ghostscript is normally used to display PostScript files and to print PostScript files to non-PostScript printers. If you need to display PostScript files or print them to non-PostScript printers, you should install ghostscript. If you install ghostscript, you also need to install the ghostscript-fonts package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

glibc-2.5-65 - glibc-2.5-81

- Group: System Environment/Libraries
- Summary: The GNU libc libraries.
- Description: The glibc package contains standard libraries which are used by multiple programs on the system. In order to save disk space and memory, as well as to make upgrading easier, common system code is kept in one place and shared between programs. This particular package contains the most important sets of shared libraries: the standard C library and the standard math library. Without these two libraries, a Linux system will not function.
- Added Dependencies:
  - systemtap-sdt-devel
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gnome-screensaver-2.16.1-8.el5_6.3 - gnome-screensaver-2.16.1-8.el5_7.5

- Group: Amusements/Graphics
- Summary: GNOME Screensaver
- Description: gnome-screensaver is a screen saver and locker that aims to have simple, sane, secure defaults and be well integrated with the desktop.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gnome-system-monitor-2.16.0-3.el5 - gnome-system-monitor-2.16.0-4.el5

- Group: Applications/System
- Summary: Simple process monitor
- Description: gnome-system-monitor is a simple process and system monitor.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gpart-0.1h-5.el5 - gpart-0.1h-6.el5

- Group: Applications/System
- Summary: A program for recovering corrupt partition tables
- Description: Gpart is a small tool which tries to guess what partitions are on a PC type harddisk in case the primary partition table was damaged.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

groff-1.18.1.1-11.1 - groff-1.18.1.1-13.el5

- Group: Applications/Publishing
- Summary: A document formatting system.
- Description: Groff is a document formatting system. Groff takes standard text and formatting commands as input and produces formatted output. The created documents can be shown on a display or printed on a printer. Groff's formatting commands allow you to specify font type and size, bold type, italic type, the number and size of columns on a page, and more. Groff can also be used to format man pages. If you are going to use groff with the X Window System, you will also need to install the groff-gxditview package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gtk2-2.10.4-21.el5_5.6 - gtk2-2.10.4-21.el5_7.7

- Group: System Environment/Libraries
- Summary: The GIMP ToolKit (GTK+), a library for creating GUIs for X
- Description: GTK+ is a multi-platform toolkit for creating graphical user interfaces. Offering a complete set of widgets, GTK+ is suitable for projects ranging from small one-off tools to complete application suites.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

hmaccalc-0.9.6-3.el5 - hmaccalc-0.9.6-4.el5

- Group: System Environment/Base
- Summary: Tools for computing and checking HMAC values for files
- Description: The hmaccalc package contains tools which can calculate HMAC (hash-based message authentication code) values for files. The names and interfaces are meant to mimic the sha*sum tools provided by the coreutils package.
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

httpd-2.2.3-53.el5 - httpd-2.2.3-63.el5

- Group: System Environment/Daemons
- Summary: Apache HTTP Server
- Description: The Apache HTTP Server is a powerful, efficient, and extensible web server.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

hwdata-0.213.24-1.el5 - hwdata-0.213.26-1.el5

- Group: System Environment/Base
- Summary: Hardware identification and configuration data
- Description: hwdata contains various hardware identification and configuration data, such as the pci.ids database and MonitorsDb databases.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ibutils-1.2-11.el5 - ibutils-1.2-11.2.el5

- Group: System Environment/Libraries
- Summary: OpenIB Mellanox InfiniBand Diagnostic Tools
- Description: ibutils provides IB network and path diagnostics.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

icu-3.6-5.16 - icu-3.6-5.16.1

- Group: System Environment/Libraries
- Summary: International Components for Unicode
- Description: The International Components for Unicode (ICU) libraries provide robust and full-featured Unicode services on a wide variety of platforms. ICU supports the most current version of the Unicode standard, and they provide support for supplementary Unicode characters (needed for GB 18030 repertoire support). As computing environments become more heterogeneous, software portability becomes more important. ICU lets you produce the same results across all the various platforms you support, without sacrificing performance. It offers great flexibility to extend and customize the supplied services.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ifd-egate-0.05-15 - ifd-egate-0.05-17.el5

- Group: System Environment/Base
- Summary: Axalto Egate SmartCard device driver for PCSC-lite
- Description: The Axalto Egate device driver enables PCSC-lite to communicate with Axalto Egate cards, which CoolKey is based off of.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

initscripts-8.45.38-2.el5 - initscripts-8.45.42-1.el5

- Group: System Environment/Base
- Summary: The inittab file and the /etc/init.d scripts.
- Description: The initscripts package contains the basic system scripts used to boot your Red Hat system, change runlevels, and shut the system down cleanly. Initscripts also

contains the scripts that activate and deactivate most network interfaces.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ipa-client-2.0-14.el5 - ipa-client-2.1.3-1.el5

- Group: System Environment/Base
- Summary: IPA authentication for use on clients
- Description: IPA is an integrated solution to provide centrally managed Identity (machine, user, virtual machines, groups, authentication credentials), Policy (configuration settings, access control information) and Audit (events, logs, analysis thereof).
- Added Dependencies:
  - curl-devel >= 7.15.5-9.el5_7.4
  - xmlrpc-c-devel >= 1.16.24-1206.1840.el5_7.3
- Removed Dependencies:
  - curl-devel
  - xmlrpc-c-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iproute-2.6.18-11.el5 - iproute-2.6.18-13.el5

- Group: Applications/System
- Summary: Advanced IP routing and network device configuration tools.
- Description: The iproute package contains networking utilities (ip and rtmon, for example) which are designed to use the advanced networking capabilities of the Linux 2.4.x and 2.6.x kernel.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iptables-1.3.5-5.3.el5_4.1 - iptables-1.3.5-9.1.el5

- Group: System Environment/Base
- Summary: Tools for managing Linux kernel packet filtering capabilities.
- Description: The iptables utility controls the network packet filtering code in the Linux kernel. If you need to set up firewalls and/or IP masquerading, you should install this package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iscsi-initiator-utils-6.2.0.872-10.el5 - iscsi-initiator-utils-6.2.0.872-13.el5

- Group: System Environment/Daemons
- Summary: iSCSI daemon and utility programs
- Description: The iscsi package provides the server daemon for the iSCSI protocol, as well as the utility programs used to manage it. iSCSI is a protocol for distributed disk access using SCSI commands sent over Internet Protocol networks.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

java-1.6.0-openjdk-1.6.0.0-1.22.1.9.8.el5_6 - java-1.6.0-openjdk-1.6.0.0-1.24.1.10.4.el5

- Group: Development/Languages
- Summary: OpenJDK Runtime Environment
- Description: The OpenJDK runtime environment.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kdeadmin-3.5.4-3.el5 - kdeadmin-3.5.4-4.el5

- Group: User Interface/Desktops
- Summary: Administrative tools for KDE.
- Description: The kdeadmin package includes administrative tools for the K Desktop Environment (KDE) including: kcron - Crontab editor kdat - Tape backup tool kuser - Frontend for configuring users and user groups
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kdebase-3.5.4-24.el5 - kdebase-3.5.4-25.el5

- Group: User Interface/Desktops
- Summary: K Desktop Environment - core files
- Description: Core applications for the K Desktop Environment. Included are: kdm (replacement for xdm), kwin (window manager), konqueror (filemanager, web browser, ftp client, ...), konsole (xterm replacement), kpanel (application starter and desktop pager), kaudio (audio server), kdehelp (viewer for kde help files, info and man pages), kthememgr (system for managing alternate theme packages) plus other KDE components (kcheckpass, kikbd, kscreensaver, kcontrol, kfind, kfontmanager, kmenuedit).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kdelibs-3.5.4-25.el5_4.1 - kdelibs-3.5.4-26.el5_7.1

- Group: System Environment/Libraries
- Summary: K Desktop Environment - Libraries
- Description: Libraries for the K Desktop Environment: KDE Libraries included: kdecore (KDE core library), kdeui (user interface), kfm (file manager), khtmlw (HTML widget), kio (Input/Output, networking), kspell (spelling checker), jscript (javascript), kab (addressbook), kimgio (image manipulation).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kdeutils-3.5.4-5.fc6 - kdeutils-3.5.4-6.el5

- Group: Applications/System
- Summary: K Desktop Environment - Utilities
- Description: Utilities for the K Desktop Environment. Includes: ark (tar/gzip archive manager); kcalc (scientific calculator); kcharselect (character selector); kdepasswd (change password); kdessh (ssh front end); kdf (view disk usage); kedit (simple text editor); kfloppy (floppy formatting tool); khexedit (hex editor); kjots (note taker); klaptopdaemon (battery monitoring and management for laptops); ksim (system information monitor); ktimer (task scheduler); kwikdisk (removable media utility)
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kernel-2.6.18-274.el5 - kernel-2.6.18-308.el5

- Group: System Environment/Kernel
- Summary: The Linux kernel (the core of the Linux operating system)
- Description: The kernel package contains the Linux kernel (vmlinuz), the core of any Linux operating system. The kernel handles the basic functions of the operating system: memory allocation, process allocation, device input and output, etc.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kexec-tools-1.102pre-126.el5_6.6 - kexec-tools-1.102pre-154.el5

- Group: Applications/System
- Summary: The kexec/kdump userspace component.
- Description: kexec-tools provides /sbin/kexec binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. This package contains the /sbin/kexec binary and ancillary utilities that together form the userspace component of

the kernel's kexec feature.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

krb5-1.6.1-62.el5 - krb5-1.6.1-70.el5

- Group: System Environment/Libraries
- Summary: The Kerberos network authentication system.
- Description: Kerberos V5 is a trusted-third-party network authentication system, which can improve your network's security by eliminating the insecure practice of cleartext passwords.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ksh-20100202-1.el5_6.6 - ksh-20100621-5.el5

- Group: Applications/Shells
- Summary: The Original ATT Korn Shell
- Description: KSH-93 is the most recent version of the KornShell by David Korn of AT&T Bell Laboratories. KornShell is a shell programming language, which is upward compatible with "sh" (the Bourne Shell).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kudzu-1.2.57.1.26-1 - kudzu-1.2.57.1.26-3

- Group: Applications/System
- Summary: The Red Hat Linux hardware probing tool.
- Description: Kudzu is a hardware probing tool run at system boot time to determine what

hardware has been added or removed from the system.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kvm-83-239.el5 - kvm-83-249.el5

- Group: Development/Tools
- Summary: Kernel-based Virtual Machine
- Description: KVM (for Kernel-based Virtual Machine) is a full virtualization solution for Linux on x86 hardware. Using KVM, one can run multiple virtual machines running unmodified Linux or Windows images. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, etc.
- Added Dependencies:
  - kernel-debug-devel = 2.6.18-304.el5
  - kernel-devel = 2.6.18-304.el5
- Removed Dependencies:
  - kernel-debug-devel = 2.6.18-269.el5
  - kernel-devel = 2.6.18-269.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

less-436-7.el5 - less-436-9.el5

- Group: Applications/Text
- Summary: A text file browser similar to more, but better.
- Description: The less utility is a text file browser that resembles more, but has more capabilities. Less allows you to move backwards in the file as well as forwards. Since less doesn't have to read the entire input file before it starts, less starts up more quickly than text editors (for example, vi). You should install less because it is a basic utility for viewing text files, and you'll use it frequently.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

lftp-3.7.11-4.el5_5.3 - lftp-3.7.11-7.el5

- Group: Applications/Internet
- Summary: A sophisticated file transfer program
- Description: LFTP is a sophisticated ftp/http file transfer program. Like bash, it has job control and uses the readline library for input. It has bookmarks, built-in mirroring, and can transfer several files in parallel. It is designed with reliability in mind.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libX11-1.0.3-11.el5 - libX11-1.0.3-11.el5_7.1

- Group: System Environment/Libraries
- Summary: X.Org X11 libX11 runtime library
- Description: X.Org X11 libX11 runtime library
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libXcursor-1.1.7-1.1 - libXcursor-1.1.7-1.2

- Group: System Environment/Libraries
- Summary: X.Org X11 libXcursor runtime library
- Description: X.Org X11 libXcursor runtime library
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libXfont-1.2.2-1.0.3.el5_1 - libXfont-1.2.2-1.0.4.el5_7

- Group: System Environment/Libraries
- Summary: X.Org X11 libXfont runtime library
- Description: X.Org X11 libXfont runtime library
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libcxgb3-1.2.5-2.el5 - libcxgb3-1.3.0-1.el5

- Group: System Environment/Libraries
- Summary: Chelsio T3 iWARP HCA Userspace Driver
- Description: Userspace hardware driver for use with the libibverbs InfiniBand/iWARP verbs library. This driver enables Chelsio iWARP capable ethernet devices.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libdhcp-1.20-11.el5 - libdhcp-1.20-13.el5

- Group: Development/Libraries
- Summary: A library for network interface configuration with DHCP
- Description: libdhcp enables programs to invoke and control the Dynamic Host Configuration Protocol (DHCP) clients: the Internet Software Consortium (ISC) IPv4 DHCP client library, libdhcp4client, and the IPv6 DHCPv6 client library, libdhcp6client, and provides Network Interface Configuration (NIC) services for network parameter autoconfiguration with DHCP.
- Added Dependencies:
  - dhcp-devel >= 12:3.0.5-31
  - libdhcp4client-devel >= 12:3.0.5-31
- Removed Dependencies:
  - dhcp-devel >= 12:3.0.5-26
  - libdhcp4client-devel >= 12:3.0.5-26
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libexif-0.6.13-4.0.2.el5_1.1 - libexif-0.6.20-1.el5_7.1

- Group: System Environment/Libraries
- Summary: Library for extracting extra information from image files
- Description: Most digital cameras produce EXIF files, which are JPEG files with extra tags that contain information about the image. The EXIF library allows you to parse an EXIF file and read the data from those tags.
- Added Dependencies:
  - pkgconfig
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libhbaapi-2.2-4.el5 - libhbaapi-2.2-6.el5

- Group: System Environment/Libraries
- Summary: SNIA HBAAPI library
- Description: The SNIA HBA API library. C-level project to manage Fibre Channel Host Bus Adapters.
- Added Dependencies:
  - autoconf
  - libtool
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libmlx4-1.0.1-6.el5 - libmlx4-1.0.1-7.el5

- Group: System Environment/Libraries
- Summary: Mellanox ConnectX InfiniBand HCA Userspace Driver
- Description: Mellanox hardware driver for use with libibverbs user space verbs access library. This driver supports Mellanox ConnectX architecture cards.
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libpng-1.2.10-7.1.el5_5.3 - libpng-1.2.10-7.1.el5_7.5

- Group: System Environment/Libraries
- Summary: A library of functions for manipulating PNG image format files
- Description: The libpng package contains a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files. PNG is a bit-mapped graphics format similar to the GIF format. PNG was created to replace the GIF format, since GIF uses a patented data compression algorithm. Libpng should be installed if you need to manipulate PNG format image files.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libusb-0.1.12-5.1 - libusb-0.1.12-6.el5

- Group: System Environment/Libraries
- Summary: A library which allows userspace access to USB devices.
- Description: This package provides a way for applications to access USB devices.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libvirt-0.8.2-22.el5 - libvirt-0.8.2-25.el5

- Group: Development/Libraries
- Summary: Library providing a simple API virtualization
- Description: Libvirt is a C toolkit to interact with the virtualization capabilities of recent versions of Linux (and other OSes).

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libxml2-2.6.26-2.1.12 - libxml2-2.6.26-2.1.12.el5_7.2

- Group: Development/Libraries
- Summary: Library providing XML and HTML support
- Description: This library allows to manipulate XML files. It includes support to read, modify and write XML and HTML files. There is DTDs support this includes parsing and validation even with complex DtDs, either at parse time or later once the document has been modified. The output can be a simple SAX stream or and in-memory DOM like representations. In this case one can use the built-in XPath and XPointer implementation to select subnodes or ranges. A flexible Input/Output mechanism is available, with existing HTTP and FTP modules and combined to an URI library.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lsof-4.78-3 - lsof-4.78-6

- Group: Development/Debuggers
- Summary: A utility which lists open files on a Linux/UNIX system.
- Description: Lsof stands for LiSt Open Files, and it does just that: it lists information about files that are open by the processes running on a UNIX system.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ltrace-0.5-13.45svn.el5 - ltrace-0.5-13.45svn.el5_7.12

- Group: Development/Debuggers
- Summary: Tracks runtime library calls from dynamically linked executables.
- Description: Ltrace is a debugging program which runs a specified command until the command exits. While the command is executing, ltrace intercepts and records both the dynamic library calls called by the executed process and the signals received by the executed process. Ltrace can also intercept and print system calls executed by the process. You should install ltrace if you need a sysadmin tool for tracking the execution of processes.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lvm2-2.02.84-6.el5 - lvm2-2.02.88-7.el5

- Group: System Environment/Base
- Summary: Userland logical volume management tools
- Description: LVM2 includes all of the support for handling read/write operations on physical volumes (hard disks, RAID-Systems, magneto optical, etc., multiple devices (MD), see mdadd(8) or even loop devices, see losetup(8)), creating volume groups (kind of virtual disks) from one or more physical volumes and creating one or more logical volumes (kind of logical partitions) in volume groups.
- Added Dependencies:
  - device-mapper >= 1.02.67-2
- Removed Dependencies:
  - device-mapper >= 1.02.63-2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

man-pages-2.39-17.el5 - man-pages-2.39-20.el5

- Group: Documentation
- Summary: Man (manual) pages from the Linux Documentation Project.
- Description: A large collection of man pages (documentation) from the Linux Documentation Project (LDP).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

man-pages-ja-20060815-14.el5 - man-pages-ja-20060815-15.el5

- Group: Documentation
- Summary: Japanese man (manual) pages from the Japanese Manual Project
- Description: Japanese Manual pages, translated by JM-Project (Japanese Manual Project).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

man-pages-overrides-0.5.7.3-3.el5 - man-pages-overrides-5.8.3-2.el5

- Group: Documentation
- Summary: Complementary and updated manual pages
- Description: A collection of manual ("man") pages to complement other packages or update those contained therein. Always have the latest version of this package installed.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mesa-6.5.1-7.8.el5 - mesa-6.5.1-7.10.el5

- Group: System Environment/Libraries
- Summary: Mesa graphics libraries
- Description: Mesa
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

microcode_ctl-1.17-1.52.el5 - microcode_ctl-1.17-1.56.el5

- Group: System Environment/Base
- Summary: Tool to update x86/x86-64 CPU microcode.
- Description: microcode_ctl - updates the microcode on Intel x86/x86-64 CPU's
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mkinitrd-5.1.19.6-71.el5 - mkinitrd-5.1.19.6-75.el5

- Group: System Environment/Base
- Summary: Creates an initial ramdisk image for preloading modules.
- Description: Mkinitrd creates filesystem images for use as initial ramdisk (initrd) images. These ramdisk images are often used to preload the block device modules (SCSI or RAID) needed to access the root filesystem. In other words, generic kernels can be built without drivers for any SCSI adapters which load the SCSI driver as a module. Since the kernel needs to read those modules, but in this case it isn't able to address the SCSI adapter, an initial ramdisk is used. The initial ramdisk is loaded by the operating system loader (normally LILO) and is available to the kernel as soon as the ramdisk is loaded. The ramdisk image loads the proper SCSI adapter and allows the kernel to mount the root filesystem. The mkinitrd program creates such a ramdisk using information found in the /etc/modules.conf file.
- Added Dependencies:
  - libdhcp-devel >= 1.20-12
- Removed Dependencies:
  - libdhcp-devel >= 1.20-6
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mktemp-1.5-23.2.2 - mktemp-1.5-24.el5

- Group: System Environment/Base
- Summary: A small utility for safely making /tmp files.
- Description: The mktemp utility takes a given file name template and overwrites a portion of

it to create a unique file name. This allows shell scripts and other programs to safely create and use /tmp files. Install the mktemp package if you need to use shell scripts or other programs which will create and use unique /tmp files.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mod_auth_kerb-5.1-3.el5 - mod_auth_kerb-5.1-3.el5_7.1

- Group: System Environment/Daemons
- Summary: Kerberos authentication module for HTTP
- Description: mod_auth_kerb is module for the Apache HTTP Server designed to provide Kerberos authentication over HTTP. The module supports the Negotiate authentication method, which performs full Kerberos authentication based on ticket exchanges.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mod_revocator-1.0.3-5.el5 - mod_revocator-1.0.3-9.el5

- Group: System Environment/Daemons
- Summary: CRL retrieval module for the Apache HTTP server
- Description: The mod_revocator module retrieves and installs remote Certificate Revocate Lists (CRLs) into an Apache web server.
- Added Dependencies:
  - autoconf
  - libtool
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mrtg-2.14.5-2 - mrtg-2.14.5-4.el5

- Group: Applications/Internet
- Summary: Multi Router Traffic Grapher
- Description: The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network-links. MRTG generates HTML pages containing PNG images which provide a LIVE visual representation of this traffic.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mysql-connector-odbc-3.51.26r1127-1.el5 - mysql-connector-odbc-3.51.26r1127-2.el5

- Group: System Environment/Libraries
- Summary: ODBC driver for MySQL
- Description: An ODBC (rev 3) driver for MySQL, for use with unixODBC.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

net-snmp-5.3.2.2-14.el5 - net-snmp-5.3.2.2-17.el5

- Group: System Environment/Daemons
- Summary: A collection of SNMP protocol tools and libraries.
- Description: SNMP (Simple Network Management Protocol) is a protocol used for network management. The NET-SNMP project includes various SNMP tools: an extensible agent, an SNMP library, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps, a version of the netstat command which uses SNMP, and a Tk/Perl mib browser. This package contains the snmpd and snmptrapd daemons, documentation, etc. You will probably also want to install the net-snmp-utils package, which contains NET-SNMP utilities. Building option: --without tcp_wrappers : disable tcp_wrappers support
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

net-tools-1.60-81.el5 - net-tools-1.60-82.el5

- Group: System Environment/Base
- Summary: Basic networking tools.
- Description: The net-tools package contains basic networking tools, including ifconfig, netstat, route, and others.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

netpbm-10.35.58-8.el5 - netpbm-10.35.58-10.el5

- Group: System Environment/Libraries
- Summary: A library for handling different graphics file formats
- Description: The netpbm package contains a library of functions which support programs for handling various graphics file formats, including .pbm (portable bitmaps), .pgm (portable graymaps), .pnm (portable anymaps), .ppm (portable pixmaps) and others.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nfs-utils-1.0.9-54.el5 - nfs-utils-1.0.9-60.el5

- Group: System Environment/Daemons
- Summary: NFS utilities and supporting clients and daemons for the kernel NFS server.
- Description: The nfs-utils package provides a daemon for the kernel NFS server and related tools, which provides a much higher level of performance than the traditional Linux NFS server used by most users. This package also contains the showmount program. Showmount queries the mount daemon on a remote host for information about the NFS (Network File System) server on the remote host. For example, showmount can display the clients which are mounted on that host. This package also contains the mount.nfs and umount.nfs program.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nfs-utils-lib-1.0.8-7.6.el5 - nfs-utils-lib-1.0.8-7.9.el5

- Group: System Environment/Libraries
- Summary: Network File System Support Library
- Description: Support libraries that are needed by the commands and daemons the nfs-utils rpm.
- Added Dependencies:
  - libtool
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nfs4-acl-tools-0.3.3-1.el5 - nfs4-acl-tools-0.3.3-3.el5

- Group: System Environment/Tools
- Summary: The nfs4 ACL tools
- Description: This package contains commandline and GUI ACL utilities for the Linux NFSv4 client.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nmap-4.11-1.1 - nmap-4.11-2

- Group: Applications/System
- Summary: Network exploration tool and security scanner
- Description: Nmap is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many port scanning techniques (determine what services the hosts are offering), and TCP/IP fingerprinting (remote host operating system identification). Nmap also offers flexible target and port specification, decoy scanning,

determination of TCP sequence predictability characteristics, reverse-identd scanning, and more.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nspr-4.8.6-1.el5 - nspr-4.8.8-2.el5

- Group: System Environment/Libraries
- Summary: Netscape Portable Runtime
- Description: NSPR provides platform independence for non-GUI operating system facilities. These facilities include threads, thread synchronization, normal file and network I/O, interval timing and calendar time, basic memory management (malloc and free) and shared library linking.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nss-3.12.8-4.el5_6 - nss-3.12.10-8.el5

- Group: System Environment/Libraries
- Summary: Network Security Services
- Description: Network Security Services (NSS) is a set of libraries designed to support cross-platform development of security-enabled client and server applications. Applications built with NSS can support SSL v2 and v3, TLS, PKCS #5, PKCS #7, PKCS #11, PKCS #12, S/MIME, X.509 v3 certificates, and other security standards.
- Added Dependencies:
  - nspr-devel >= 4.8.8
- Removed Dependencies:
  - nspr-devel >= 4.8.6
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nss_ldap-253-42.el5 - nss_ldap-253-49.el5

- Group: System Environment/Base
- Summary: NSS library and PAM module for LDAP.
- Description: This package includes two LDAP access clients: nss_ldap and pam_ldap. Nss_ldap is a set of C library extensions that allow X.500 and LDAP directory servers to be used as a primary source of aliases, ethers, groups, hosts, networks, protocol, users, RPCs, services, and shadow passwords (instead of or in addition to using flat files or NIS). Pam_ldap is a module for Linux-PAM that supports password changes, V2 clients, Netscape's SSL, ypldapd, Netscape Directory Server password policies, access authorization, and crypted hashes.
- Added Dependencies:
  - openldap-devel >= 2.3.43-20
- Removed Dependencies:
  - openldap-devel >= 2.3.43-7
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ntp-4.2.2p1-15.el5 - ntp-4.2.2p1-15.el5_7.1

- Group: System Environment/Daemons
- Summary: Synchronizes system time using the Network Time Protocol (NTP).
- Description: The Network Time Protocol (NTP) is used to synchronize a computer's time with another reference time source. The ntp package contains utilities and daemons that will synchronize your computer's time to Coordinated Universal Time (UTC) via the NTP protocol and NTP servers. The ntp package includes ntpdate (a program for retrieving the date and time from remote machines via a network) and ntpd (a daemon which continuously adjusts system time). Install the ntp package if you need tools for keeping your system's time synchronized via the NTP protocol.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

oddjob-0.27-11.el5 - oddjob-0.27-12.el5

- Group: System Environment/Daemons
- Summary: A D-BUS service which runs odd jobs on behalf of client applications
- Description: oddjob is a D-BUS service which performs particular tasks for clients which

connect to it and issue requests using the system-wide message bus.

- Added Dependencies:
  - autoconf
  - automake
  - libtool
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openCryptoki-2.2.4-22.el5_5.1 - openCryptoki-2.2.4-25.el5

- Group: Productivity/Security
- Summary: Implementation of Cryptoki v2.11 for IBM Crypto Hardware
- Description: The PKCS#11 Version 2.11 api implemented for the IBM Crypto cards. This package includes support for the IBM 4758 Cryptographic CoProcessor (with the PKCS#11 firmware loaded) and the IBM eServer Cryptographic Accelerator (FC 4960 on pSeries)
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openais-0.80.6-30.el5 - openais-0.80.6-36.el5

- Group: System Environment/Base
- Summary: The openais Standards-Based Cluster Framework executive and APIs
- Description: This package contains the openais executive, openais service handlers, default configuration files and init script.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openldap-2.3.43-12.el5_6.7 - openldap-2.3.43-25.el5

- Group: System Environment/Daemons
- Summary: The configuration files, libraries, and documentation for OpenLDAP.
- Description: OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. LDAP is a set of protocols for accessing directory services (usually phone book style information, but other information is possible) over the Internet, similar to the way DNS (Domain Name System) information is propagated over the Internet. The openldap package contains configuration files, libraries, and documentation for OpenLDAP.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openmotif-2.3.1-5.el5_5.1 - openmotif-2.3.1-6.el5

- Group: System Environment/Libraries
- Summary: Open Motif runtime libraries and executables.
- Description: This is the Open Motif 2.3.1 runtime environment. It includes the Motif shared libraries, needed to run applications which are dynamically linked against Motif, and the Motif Window Manager "mwm".
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openmotif22-2.2.3-18 - openmotif22-2.2.3-20

- Group: System Environment/Libraries
- Summary: Open Motif runtime libraries and executables
- Description: This is the Open Motif 2.2.3 runtime environment. It includes the Motif shared libraries, needed to run applications which are dynamically linked against Motif.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

openscap-0.7.2-1.el5 - openscap-0.8.0-1.el5

- Group: System Environment/Libraries
- Summary: Set of open source libraries enabling integration of the SCAP line of standards
- Description: OpenSCAP is a set of open source libraries providing an easier path for integration of the SCAP line of standards. SCAP is a line of standards managed by NIST with the goal of providing a standard language for the expression of Computer Network Defense related information.
- Added Dependencies:
  - GConf2-devel
  - libcap-devel
  - libnl-devel
  - libselinux-devel
  - openldap-devel
- Removed Dependencies:
  - curl-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openssh-4.3p2-72.el5_6.3 - openssh-4.3p2-82.el5

- Group: Applications/Internet
- Summary: The OpenSSH implementation of SSH protocol versions 1 and 2
- Description: SSH (Secure SHell) is a program for logging into and executing commands on a remote machine. SSH is intended to replace rlogin and rsh, and to provide secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel. OpenSSH is OpenBSD's version of the last free version of SSH, bringing it up to date in terms of security and features, as well as removing all patented algorithms to separate libraries. This package includes the core files necessary for both the OpenSSH client and server. To make this package useful, you should also install openssh-clients, openssh-server, or both.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openssl-0.9.8e-20.el5 - openssl-0.9.8e-22.el5

- Group: System Environment/Libraries
- Summary: The OpenSSL toolkit
- Description: The OpenSSL toolkit provides support for secure communications between machines. OpenSSL includes a certificate management tool and shared libraries which provide various cryptographic algorithms and protocols.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openswan-2.6.21-5.el5_6.4 - openswan-2.6.32-3.el5

- Group: System Environment/Daemons
- Summary: IPSEC implementation with IKEv1 and IKEv2 keying protocols
- Description: Openswan is a free implementation of IPsec & IKE for Linux. IPsec is the Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks. Everything passing through the untrusted net is encrypted by the ipsec gateway machine and decrypted by the gateway at the other end of the tunnel. The resulting tunnel is a virtual private network or VPN. This package contains the daemons and userland tools for setting up Openswan. It supports the NETKEY/XFRM IPsec kernel stack that exists in the default Linux kernel. Openswan 2.6.x also supports IKEv2 (RFC4306)
- Added Dependencies:
  - curl-devel
  - libselinux-devel
  - openldap-devel
- Removed Dependencies:
  - man
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

oprofile-0.9.4-15.el5 - oprofile-0.9.4-20.el5

- Group: Development/System
- Summary: System wide profiler
- Description: OProfile is a profiling system for systems running Linux. The profiling runs transparently during the background, and profile data can be collected at any time. OProfile

makes use of the hardware performance counters provided on Intel P6, and AMD Athlon family processors, and can use the RTC for profiling on other x86 processor types. See the HTML documentation for further details.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pam_krb5-2.2.14-21.el5 - pam_krb5-2.2.14-22.el5

- Group: System Environment/Base
- Summary: A Pluggable Authentication Module for Kerberos 5.
- Description: This is pam_krb5, a pluggable authentication module that can be used with Linux-PAM and Kerberos 5. This module supports password checking, ticket creation, and optional TGT verification and conversion to Kerberos IV tickets. The included pam_krb5afs module also gets AFS tokens if so configured.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pam_pkcs11-0.5.3-23 - pam_pkcs11-0.5.3-26.el5

- Group: System Environment/Base
- Summary: PKCS #11/NSS PAM login module
- Description: This Linux-PAM login module allows a X.509 certificate based user authentication. The certificate and its dedicated private key are thereby accessed by means of an appropriate PKCS #11 module. For the verification of the users' certificates, locally stored CA certificates as well as either online or locally accessible CRLs and OCSP are used. This version uses NSS to validate the Certificates and manage the PKCS #11 smartCards. Additional included pam_pkcs11 related tools - pkcs11_eventmgr: Generate actions on card insert/removal/timeout events - pklogin_finder: Get the loginname that maps to a certificate - pkcs11_inspect: Inspect the contents of a certificate
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

pango-1.14.9-8.el5_6.2 - pango-1.14.9-8.el5_7.3

- Group: System Environment/Libraries
- Summary: System for layout and rendering of internationalized text
- Description: Pango is a system for layout and rendering of internationalized text.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

parted-1.8.1-28.el5 - parted-1.8.1-29.el5

- Group: Applications/System
- Summary: The GNU disk partition manipulation program
- Description: The GNU Parted program allows you to create, destroy, resize, move, and copy hard disk partitions. Parted can be used for creating space for new operating systems, reorganizing disk usage, and copying data to new hard disks.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pciutils-3.1.7-3.el5 - pciutils-3.1.7-5.el5

- Group: Applications/System
- Summary: PCI bus related utilities
- Description: The pciutils package contains various utilities for inspecting and setting devices connected to the PCI bus. The utilities provided require kernel version 2.1.82 or newer (which support the /proc/bus/pci interface).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

pdksh-5.2.14-36.el5 - pdksh-5.2.14-37.el5

- Group: System Environment/Shells
- Summary: A public domain shell implementing ksh-88
- Description: The pdksh package contains public domain implementation of ksh-88. The ksh shell is a command interpreter intended for both interactive and shell script use. Ksh's command language is a superset of the sh shell language. Pdksh is unmaintained since 1998 and is obsoleted by ksh package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

perl-5.8.8-32.el5_6.3 - perl-5.8.8-38.el5

- Group: Development/Languages
- Summary: The Perl programming language
- Description: Perl is a high-level programming language with roots in C, sed, awk and shell scripting. Perl is good at handling processes and files, and is especially good at handling text. Perl's hallmarks are practicality and efficiency. While it is used to do a lot of different things, Perl's most common applications are system administration utilities and web programming. A large proportion of the CGI scripts on the web are written in Perl. You need the perl package installed on your system so that your system can handle Perl scripts. Install this package if you want to program in Perl or enable your system to handle Perl scripts.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

perl-XML-SAX-0.14-8 - perl-XML-SAX-0.14-11

- Group: Development/Libraries
- Summary: XML-SAX Perl module
- Description: XML-SAX Perl module.
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

php-5.1.6-27.el5_5.3 - php-5.1.6-32.el5

- Group: Development/Languages
- Summary: The PHP HTML-embedded scripting language. (PHP: Hypertext Preprocessor)
- Description: PHP is an HTML-embedded scripting language that allows developers to write dynamically generated web pages. PHP is ideal for writing database-enabled websites, with built-in integration for several commercial and non-commercial database management systems. PHP is often used as a replacement for CGI scripts. The php package contains a module that adds support for the PHP language to the Apache HTTP Server.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

php-pear-1.4.9-6.el5 - php-pear-1.4.9-8.el5

- Group: System
- Summary: PHP Extension and Application Repository framework
- Description: PEAR is a framework and distribution system for reusable PHP components. This package contains the basic PEAR components.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

php53-5.3.3-1.el5_6.1 - php53-5.3.3-5.el5

- Group: Development/Languages
- Summary: PHP scripting language for creating dynamic web sites
- Description: PHP is an HTML-embedded scripting language. PHP attempts to make it easy

for developers to write dynamically generated webpages. PHP also offers built-in database integration for several commercial and non-commercial database management systems, so writing a database-enabled webpage with PHP is fairly simple. The most common use of PHP coding is probably as a replacement for CGI scripts. The php package contains the module which adds support for the PHP language to Apache HTTP Server.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pidgin-2.6.6-5.el5_5 - pidgin-2.6.6-5.el5_7.4

- Group: Applications/Internet
- Summary: A Gtk+ based multiprotocol instant messaging client
- Description: Pidgin allows you to talk to anyone using a variety of messaging protocols including AIM, MSN, Yahoo!, Jabber, Bonjour, Gadu-Gadu, ICQ, IRC, Novell Groupwise, QQ, Lotus Sametime, SILC, Simple and Zephyr. These protocols are implemented using a modular, easy to use design. To use a protocol, just add an account using the account editor. Pidgin supports many common features of other clients, as well as many unique features, such as perl scripting, TCL scripting and C plugins. Pidgin is not affiliated with or endorsed by America Online, Inc., Microsoft Corporation, Yahoo! Inc., or ICQ Inc.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

poppler-0.5.4-4.4.el5_6.17 - poppler-0.5.4-19.el5

- Group: Development/Libraries
- Summary: PDF rendering library
- Description: Poppler, a PDF rendering library, it's a fork of the xpdf PDF viewer developed by Derek Noonburg of Glyph and Cog, LLC.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

postgresql-8.1.23-1.el5_6.1 - postgresql-8.1.23-1.el5_7.3

- Group: Applications/Databases
- Summary: PostgreSQL client programs and libraries.
- Description: PostgreSQL is an advanced Object-Relational database management system (DBMS) that supports almost all SQL constructs (including transactions, subselects and user-defined types and functions). The postgresql package includes the client programs and libraries that you'll need to access a PostgreSQL DBMS server. These PostgreSQL client programs are programs that directly manipulate the internal structure of PostgreSQL databases on a PostgreSQL server. These client programs can be located on the same machine with the PostgreSQL server, or may be on a remote machine which accesses a PostgreSQL server over a network connection. This package contains the docs in HTML for the whole package, as well as command-line utilities for managing PostgreSQL databases on a PostgreSQL server. If you want to manipulate a PostgreSQL database on a remote PostgreSQL server, you need this package. You also need to install this package if you're installing the postgresql-server package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

postgresql84-8.4.7-1.el5_6.1 - postgresql84-8.4.9-1.el5_7.1

- Group: Applications/Databases
- Summary: PostgreSQL client programs
- Description: PostgreSQL is an advanced Object-Relational database management system (DBMS) that supports almost all SQL constructs (including transactions, subselects and user-defined types and functions). The postgresql package includes the client programs and libraries that you'll need to access a PostgreSQL DBMS server. These PostgreSQL client programs are programs that directly manipulate the internal structure of PostgreSQL databases on a PostgreSQL server. These client programs can be located on the same machine with the PostgreSQL server, or may be on a remote machine which accesses a PostgreSQL server over a network connection. This package contains the docs in HTML for the whole package, as well as command-line utilities for managing PostgreSQL databases on a PostgreSQL server. If you want to manipulate a PostgreSQL database on a local or remote PostgreSQL server, you need this package. You also need to install this package if you're installing the postgresql-server package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

procinfo-18-19 - procinfo-18-19.el5_7.2

- Group: Applications/System
- Summary: A tool for gathering and displaying system information.
- Description: The procinfo command gets system data from the /proc directory (the kernel filesystem), formats it and displays it on standard output. You can use procinfo to acquire information about your system from the kernel as it is running. Install procinfo if you'd like to use it to gather and display system data.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

procps-3.2.7-17.el5 - procps-3.2.7-18.el5

- Group: Applications/System
- Summary: System and process monitoring utilities.
- Description: The procps package contains a set of system utilities that provide system information. Procps includes ps, free, skill, pkill, pgrep, snice, tload, top, uptime, vmstat, w, watch and pdwx. The ps command displays a snapshot of running processes. The top command provides a repetitive update of the statuses of running processes. The free command displays the amounts of free and used memory on your system. The skill command sends a terminate command (or another specified signal) to a specified set of processes. The snice command is used to change the scheduling priority of specified processes. The tload command prints a graph of the current system load average to a specified tty. The uptime command displays the current time, how long the system has been running, how many users are logged on, and system load averages for the past one, five, and fifteen minutes. The w command displays a list of the users who are currently logged on and what they are running. The watch program watches a running program. The vmstat command displays virtual memory statistics about processes, memory, paging, block I/O, traps, and CPU activity. The pwdx command reports the current working directory of a process or processes.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

python-2.4.3-44.el5 - python-2.4.3-46.el5

- Group: Development/Languages
- Summary: An interpreted, interactive, object-oriented programming language.
- Description: Python is an interpreted, interactive, object-oriented programming language often compared to Tcl, Perl, Scheme or Java. Python includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems (X11, Motif, Tk, Mac and MFC). Programmers can write new built-in modules for Python in C or C++. Python can be used as an extension language for applications that need a programmable interface. This package contains most of the standard Python modules, as well as modules for interfacing to the Tix widget set for Tk and RPM. Note that documentation for Python is provided in the python-docs package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

python-rhsm-0.95.5.5-1.el5 - python-rhsm-0.98.9-1.el5

- Group: Development/Libraries
- Summary: A Python library to communicate with a Red Hat Unified Entitlement Platform
- Description: A small library for communicating with the REST interface of a Red Hat Unified Entitlement Platform. This interface is used for the management of system entitlements, certificates, and access to content.
- Added Dependencies:
  - rpm-python
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

python-virtinst-0.400.3-12.el5 - python-virtinst-0.400.3-13.el5

- Group: Development/Libraries
- Summary: Python modules and utilities for installing virtual machines
- Description: virtinst is a module that helps build and install libvirt based virtual machines. Currently supports KVM, QEmu and Xen virtual machines. Package includes several command line utilities, including virt-install (build and install new VMs) and virt-clone (clone an existing virtual machine).

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pyxf86config-0.3.31-2.fc6 - pyxf86config-0.3.31-3.el5

- Group: System Environment/Libraries
- Summary: Python wrappers for libxf86config
- Description: Python wrappers for the X server config file library libxf86config. It is used to read and write X server configuration files.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

qt-3.3.6-23.el5 - qt-3.3.6-25.el5

- Group: System Environment/Libraries
- Summary: The shared library for the Qt GUI toolkit.
- Description: Qt is a GUI software toolkit which simplifies the task of writing and maintaining GUI (Graphical User Interface) applications for the X Window System. Qt is written in C++ and is fully object-oriented. This package contains the shared library needed to run qt applications, as well as the README files for qt.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

qt4-4.2.1-1 - qt4-4.2.1-1.el5_7.1

- Group: System Environment/Libraries
- Summary: The shared library for the Qt GUI toolkit
- Description: Qt is a GUI software toolkit which simplifies the task of writing and maintaining

GUI (Graphical User Interface) applications for the X Window System. Qt is written in C++ and is fully object-oriented. This package contains the shared library needed to run qt applications, as well as the README files for qt.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rdesktop-1.6.0-3.el5_6.2 - rdesktop-1.6.0-7

- Group: User Interface/Desktops
- Summary: X client for remote desktop into Windows Terminal Server
- Description: rdesktop is an open source client for Windows NT Terminal Server and Windows 2000 & 2003 Terminal Services, capable of natively speaking Remote Desktop Protocol (RDP) in order to present the user's NT desktop. Unlike Citrix ICA, no server extensions are required.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

redhat-release-5Client-5.7.0.3 - redhat-release-5Client-5.8.0.3

- Group: System Environment/Base
- Summary: Red Hat Enterprise Linux release file
- Description: Red Hat Enterprise Linux release files
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

redhat-release-notes-5Client-41 - redhat-release-notes-5Client-43

- Group: System Environment/Base

- Summary: Red Hat Enterprise Linux release notes files
- Description: Red Hat Enterprise Linux release notes files.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhn-client-tools-0.4.20-56.el5 - rhn-client-tools-0.4.20-77.el5

- Group: System Environment/Base
- Summary: Support programs and libraries for Red Hat Network
- Description: Red Hat Network Client Tools provides programs and libraries to allow your system to receive software updates from Red Hat Network.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhnlib-2.5.22-6.el5 - rhnlib-2.5.22-7.el5

- Group: Development/Libraries
- Summary: Python libraries for the RHN project
- Description: rhnlib is a collection of python modules used by the Red Hat Network (http://rhn.redhat.com) software.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhpl-0.194.1-1 - rhpl-0.194.1-2

- Group: System Environment/Libraries
- Summary: Library of python code used by programs in Red Hat Linux
- Description: The rhpl package contains Python code used by programs in Red Hat Linux.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhpxl-0.41.1-9.el5 - rhpxl-0.41.1-12.el5

- Group: System Environment/Libraries
- Summary: Python library for configuring and running X.
- Description: The rhpxl (pronounced 'rapunzel') package contains a Python library for configuring and running X.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rng-utils-2.0-4.el5 - rng-utils-2.0-5.el5

- Group: System Environment/Base
- Summary: Random number generator related utilities
- Description: Hardware random number generation tools.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rpm-4.4.2.3-22.el5 - rpm-4.4.2.3-27.el5

- Group: System Environment/Base
- Summary: The RPM package management system
- Description: The RPM Package Manager (RPM) is a powerful command line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages. Each software package consists of an archive of files along with information about the package like its version, a description, etc.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rsh-0.17-40.el5 - rsh-0.17-40.el5_7.1

- Group: Applications/Internet
- Summary: Clients for remote access commands (rsh, rlogin, rcp).
- Description: The rsh package contains a set of programs which allow users to run commands on remote machines, login to other machines and copy files between machines (rsh, rlogin and rcp). All three of these commands use rhosts style authentication. This package contains the clients needed for all of these services. The rsh package should be installed to enable remote access to other machines.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rsync-3.0.6-4.el5 - rsync-3.0.6-4.el5_7.1

- Group: Applications/Internet
- Summary: A program for synchronizing files over a network
- Description: Rsync uses a reliable algorithm to bring remote and host files into sync very quickly. Rsync is fast because it just sends the differences in the files over the network instead of sending the complete files. Rsync is often used as a very powerful mirroring process or just as a more capable replacement for the rcp command. A technical report which describes the rsync algorithm is included in this package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rsyslog-3.22.1-3.el5_6.1 - rsyslog-3.22.1-7.el5

- Group: System Environment/Daemons
- Summary: Enhanced system logging and kernel message trapping daemon
- Description: Rsyslog is an enhanced, multi-threaded syslog daemon. It supports MySQL, syslog/TCP, RFC 3195, permitted sender lists, filtering on any message part, and fine grain output format control. It is compatible with stock sysklogd and can be used as a drop-in replacement. Rsyslog is simple to set up, with advanced features suitable for enterprise-class, encryption-protected syslog relay chains.
- Added Dependencies:
  - net-snmp-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ruby-1.8.5-19.el5_6.1 - ruby-1.8.5-24.el5

- Group: Development/Languages
- Summary: An interpreter of object-oriented scripting language
- Description: Ruby is the interpreted scripting language for quick and easy object-oriented programming. It has many features to process text files and to do system management tasks (as in Perl). It is simple, straight-forward, and extensible.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sabayon-2.12.4-7.el5 - sabayon-2.12.4-9.el5

- Group: Applications/System
- Summary: Tool to maintain user profiles in a GNOME desktop
- Description: Sabayon is a tool to help sysadmins and user change and maintain the default behaviour of the GNOME desktop. This package contains the graphical tools which a sysadmin use to manage Sabayon profiles.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

samba-3.0.33-3.29.el5_6.2 - samba-3.0.33-3.37.el5

- Group: System Environment/Daemons
- Summary: The Samba SMB server.
- Description: Samba is the suite of programs by which a lot of PC-related machines share files, printers, and other information (such as lists of available files and printers). The Windows NT, OS/2, and Linux operating systems support this natively, and add-on packages can enable the same thing for DOS, Windows, VMS, UNIX of all kinds, MVS, and more. This package provides an SMB server that can be used to provide network services to SMB (sometimes called "Lan Manager") clients. Samba uses NetBIOS over TCP/IP (NetBT) protocols and does NOT need the NetBEUI (Microsoft Raw NetBIOS frame) protocol.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

samba3x-3.5.4-0.83.el5 - samba3x-3.5.10-0.107.el5

- Group: System Environment/Daemons
- Summary: Server and Client software to interoperate with Windows machines
- Description: Samba is the suite of programs by which a lot of PC-related machines share files, printers, and other information (such as lists of available files and printers). The Windows NT, OS/2, and Linux operating systems support this natively, and add-on packages can enable the same thing for DOS, Windows, VMS, UNIX of all kinds, MVS, and more. This package provides an SMB/CIFS server that can be used to provide network services to SMB/CIFS clients. Samba uses NetBIOS over TCP/IP (NetBT) protocols and does NOT need the NetBEUI (Microsoft Raw NetBIOS frame) protocol.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sblim-1-47.el5 - sblim-1-49.el5

- Group: Applications/System
- Summary: Standards Based Linux Instrumentation for Manageability

- Description: SBLIM stands for Standards Based Linux Instrumentation for Manageability, and consists of a set of standards based Web Based Enterprise Management (WBEM) modules that use the Common Information Model (CIM) standard to gather and provide systems management information, events, and methods to local or networked consumers via an CIM object services broker using the CMPI (Common Manageability Programming Interface) standard. This package provides a set of core providers and development tools for systems management applications.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

scim-bridge-0.4.5-9.el5 - scim-bridge-0.4.5-10.el5

- Group: System Environment/Libraries
- Summary: SCIM Bridge Gtk IM module
- Description: SCIM Bridge is a C implementation of a Gtk IM module for SCIM.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

selinux-policy-2.4.6-316.el5 - selinux-policy-2.4.6-327.el5

- Group: System Environment/Base
- Summary: SELinux policy configuration
- Description: SELinux Reference Policy - modular.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sendmail-8.13.8-8.el5 - sendmail-8.13.8-8.1.el5_7

- Group: System Environment/Daemons
- Summary: A widely used Mail Transport Agent (MTA).
- Description: The Sendmail program is a very widely used Mail Transport Agent (MTA). MTAs send mail from one machine to another. Sendmail is not a client program, which you use to read your email. Sendmail is a behind-the-scenes program which actually moves your email over networks or the Internet to where you want it to go. If you ever need to reconfigure Sendmail, you will also need to have the sendmail.cf package installed. If you need documentation on Sendmail, you can install the sendmail-doc package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

setup-2.5.58-7.el5 - setup-2.5.58-9.el5

- Group: System Environment/Base
- Summary: A set of system configuration and setup files.
- Description: The setup package contains a set of important system configuration and setup files, such as passwd, group, and profile.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

shadow-utils-4.0.17-18.el5_6.1 - shadow-utils-4.0.17-20.el5

- Group: System Environment/Base
- Summary: Utilities for managing accounts and shadow password files.
- Description: The shadow-utils package includes the necessary programs for converting UNIX password files to the shadow password format, plus programs for managing user and group accounts. The pwconv command converts passwords to the shadow password format. The pwunconv command unconverts shadow passwords and generates an npasswd file (a standard UNIX password file). The pwck command checks the integrity of password and shadow files. The lastlog command prints out the last login times for all users. The useradd, userdel, and usermod commands are used for managing user accounts. The groupadd, groupdel, and groupmod commands are used for managing group accounts.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

smartmontools-5.38-2.el5 - smartmontools-5.38-3.el5

- Group: System Environment/Base
- Summary: Tools for monitoring SMART capable hard disks
- Description: The smartmontools package contains two utility programs (smartctl and smartd) to control and monitor storage systems using the Self- Monitoring, Analysis and Reporting Technology System (SMART) built into most modern ATA and SCSI hard disks. In many cases, these utilities will provide advanced warning of disk degradation and failure.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sos-1.7-9.54.el5 - sos-1.7-9.62.el5

- Group: Development/Libraries
- Summary: A set of tools to gather troubleshooting information from a system
- Description: Sos is a set of tools that gathers information about system hardware and configuration. The information can then be used for diagnostic purposes and debugging. Sos is commonly used to help support technicians and developers.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

spice-xpi-2.2-2.3.el5_6.1 - spice-xpi-2.4-4.el5

- Group: Applications/Internet
- Summary: SPICE extension for Mozilla
- Description: SPICE extension for mozilla allows the client to be used from a web browser.
- Added Dependencies:

    - autoconf
    - libtool
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sssd-1.5.1-37.el5 - sssd-1.5.1-49.el5

- Group: Applications/System
- Summary: System Security Services Daemon
- Description: Provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides an NSS and PAM interface toward the system and a pluggable backend system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects like FreeIPA.
- Added Dependencies:
    - diffstat
    - findutils
    - glib2-devel
    - pkgconfig
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

subscription-manager-0.95.5.21-1.el5 - subscription-manager-0.98.14-1.el5

- Group: System Environment/Base
- Summary: Tools and libraries for subscription and repository management
- Description: The Subscription Manager package provides programs and libraries to allow users to manage subscriptions and yum repositories from the Red Hat entitlement platform.
- Added Dependencies:
    - scrollkeeper
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

sudo-1.7.2p1-10.el5 - sudo-1.7.2p1-13.el5

- Group: Applications/System
- Summary: Allows restricted root access for specified users.
- Description: Sudo (superuser do) allows a system administrator to give certain users (or groups of users) the ability to run some (or all) commands as root while logging all commands and arguments. Sudo operates on a per-command basis. It is not a replacement for the shell. Features include: the ability to restrict what commands a user may run on a per-host basis, copious logging of each command (providing a clear audit trail of who did what), a configurable timeout of the sudo command, and the ability to use the same configuration file (sudoers) on many different machines.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

switchdesk-4.0.8-6 - switchdesk-4.0.8-7.el5

- Group: User Interface/Desktops
- Summary: A desktop environment switcher for GNOME, KDE and AnotherLevel.
- Description: The Desktop Switcher is a tool which enables users to easily switch between various desktop environments that they have installed. The tool includes support for KDE, GNOME, XFce4 and twm. Support for different environments on different computers is available, as well as support for setting a global default environment. Install switchdesk if you need a tool for switching between desktop environments.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

syslinux-3.11-4 - syslinux-3.11-7

- Group: Applications/System
- Summary: Simple kernel loader which boots from a FAT filesystem
- Description: SYSLINUX is a suite of bootloaders, currently supporting DOS FAT filesystems, Linux ext2/ext3 filesystems (EXTLINUX), PXE network boots (PXELINUX), or ISO 9660 CD-ROMs (ISOLINUX). It also includes a tool, MEMDISK, which loads legacy operating systems from these media.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-bind-4.0.3-4.el5 - system-config-bind-4.0.3-5.el5

- Group: Applications/System
- Summary: The Red Hat BIND DNS Configuration Tool.
- Description: The system-config-bind package provides a graphical user interface (GUI) to configure the Berkeley Internet Name Domain (BIND) Domain Name System (DNS) server, "named", with a set of python modules. Users new to BIND configuration can use this tool to quickly set up a working DNS server.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-date-1.8.12-4.el5 - system-config-date-1.8.12-5.el5

- Group: System Environment/Base
- Summary: A graphical interface for modifying system date and time
- Description: system-config-date is a graphical interface for changing the system date and time, configuring the system time zone, and setting up the NTP daemon to synchronize the time of the system with an NTP time server.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-display-1.0.48-2.el5 - system-config-display-1.0.48-4.el5

- Group: System Environment/Base
- Summary: A graphical interface for configuring the X Window System display

- Description: system-config-display is a graphical application for configuring an X Window System X server display.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-network-1.3.99.19-2.el5 - system-config-network-1.3.99.21-1.el5

- Group: Applications/System
- Summary: The GUI of the NEtwork Adminstration Tool
- Description: This is the GUI of the network configuration tool, supporting Ethernet, Wireless, TokenRing, ADSL, ISDN and PPP.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-nfs-1.3.23-1.el5 - system-config-nfs-1.3.23-2.el5

- Group: System Environment/Base
- Summary: NFS server configuration tool
- Description: system-config-nfs is a graphical user interface for creating, modifying, and deleting nfs shares.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-printer-0.7.32.10-1.el5 - system-config-printer-0.7.32.10-1.el5_7.1

- Group: System Environment/Base
- Summary: A printer administration tool
- Description: system-config-printer is a graphical user interface that allows the user to

configure a CUPS print server.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-users-1.2.51-4.el5 - system-config-users-1.2.51-7.el5

- Group: Applications/System
- Summary: A graphical interface for administering users and groups
- Description: system-config-users is a graphical utility for administrating users and groups. It depends on the libuser library.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-switch-mail-0.5.25-12 - system-switch-mail-0.5.25-13.el5

- Group: Applications/System
- Summary: The Mail Transport Agent Switcher
- Description: The system-switch-mail is the Mail Transport Agent Switcher. It enables users to easily switch between various Mail Transport Agent that they have installed.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

systemtap-1.3-8.el5 - systemtap-1.6-6.el5

- Group: Development/System
- Summary: Instrumentation System
- Description: SystemTap is an instrumentation system for systems running Linux. Developers can write instrumentation to collect data on the operation of the system.

- Added Dependencies:
  - gettext
  - gettext-devel
- Removed Dependencies:
  - nss-tools
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tar-1.15.1-30.el5 - tar-1.15.1-31.el5

- Group: Applications/Archiving
- Summary: A GNU file archiving program
- Description: The GNU tar program saves many files together in one archive and can restore individual files (or all of the files) from that archive. Tar can also be used to add supplemental files to an archive and to update or list files in the archive. Tar includes multivolume support, automatic archive compression/decompression, the ability to perform remote archives, and the ability to perform incremental and full backups. If you want to use tar for remote backups, you also need to install the rmt package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

thunderbird-2.0.0.24-18.el5_6 - thunderbird-2.0.0.24-28.el5_7

- Group: Applications/Internet
- Summary: Mozilla Thunderbird mail/newsgroup client
- Description: Mozilla Thunderbird is a standalone mail and newsgroup client.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tog-pegasus-2.9.1-2.el5_5.1 - tog-pegasus-2.11.0-3.el5

- Group: Systems Management/Base
- Summary: OpenPegasus WBEM Services for Linux
- Description: OpenPegasus WBEM Services for Linux enables management solutions that deliver increased control of enterprise resources. WBEM is a platform and resource independent DMTF standard that defines a common information model and communication protocol for monitoring and controlling resources from diverse sources.
- Added Dependencies:
  - rpm
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tomcat5-5.5.23-0jpp.19.el5_6 - tomcat5-5.5.23-0jpp.22.el5_7

- Group: Networking/Daemons
- Summary: Apache Servlet/JSP Engine, RI for Servlet 2.4/JSP 2.0 API
- Description: Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies. The Java Servlet and JavaServer Pages specifications are developed by Sun under the Java Community Process. Tomcat is developed in an open and participatory environment and released under the Apache Software License. Tomcat is intended to be a collaboration of the best-of-breed developers from around the world. We invite you to participate in this open development project. To learn more about getting involved, click here.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tzdata-2011g-1.el5 - tzdata-2011l-4.el5

- Group: System Environment/Base
- Summary: Timezone data
- Description: This package contains data files with rules for various time zones around the world.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

udev-095-14.27.el5 - udev-095-14.27.el5_7.1

- Group: System Environment/Base
- Summary: A userspace implementation of devfs
- Description: The udev package contains an implementation of devfs in userspace using sysfs and netlink.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

unixODBC-2.2.11-7.1 - unixODBC-2.2.11-10.el5

- Group: System Environment/Libraries
- Summary: A complete ODBC driver manager for Linux
- Description: Install unixODBC if you want to access databases through ODBC. This package includes low-level drivers for MySQL, PostgreSQL, and local files. However, the included drivers are not as up-to-date as the ones distributed separately. It is recommended that you install and use the MyODBC package if you need a driver for MySQL, and/or the postgresql-odbc package for PostgreSQL.
- Added Dependencies:
  - libtool >= 1.5.22-7
- Removed Dependencies:
  - libtool
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

util-linux-2.13-0.56.el5 - util-linux-2.13-0.59.el5

- Group: System Environment/Base
- Summary: A collection of basic system utilities.
- Description: The util-linux package contains a large variety of low-level system utilities that

are necessary for a Linux system to function. Among others, Util-linux contains the fdisk configuration tool and the login program.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

virt-manager-0.6.1-14.el5 - virt-manager-0.6.1-16.el5

- Group: Applications/Emulators
- Summary: Virtual Machine Manager
- Description: Virtual Machine Manager provides a graphical tool for administering virtual machines for KVM, Xen, and QEmu. Start, stop, add or remove virtual devices, connect to a graphical or serial console, and see resource usage statistics for existing VMs on local or remote machines. Uses libvirt as the backend management API.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

vixie-cron-4.1-77.el5_4.1 - vixie-cron-4.1-81.el5

- Group: System Environment/Base
- Summary: The Vixie cron daemon for executing specified programs at set times.
- Description: The vixie-cron package contains the Vixie version of cron. Cron is a standard UNIX daemon that runs specified programs at scheduled times. Vixie cron adds better security and more powerful configuration options to the standard version of cron.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

vsftpd-2.0.5-21.el5 - vsftpd-2.0.5-24.el5

- Group: System Environment/Daemons
- Summary: vsftpd - Very Secure Ftp Daemon
- Description: vsftpd is a Very Secure FTP daemon. It was written completely from scratch.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xen-3.0.3-132.el5 - xen-3.0.3-135.el5

- Group: Development/Libraries
- Summary: Xen is a virtual machine monitor
- Description: This package contains the Xen tools and management daemons needed to run virtual machines on x86, x86_64, and ia64 systems. Information on how to use Xen can be found at the Xen project pages. The Xen system also requires the Xen hypervisor and domain-0 kernel, which can be found in the kernel-xen* package. Virtualization can be used to run multiple operating systems on one physical system, for purposes of hardware consolidation, hardware abstraction, or to test untrusted applications in a sandboxed environment.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xinetd-2.3.14-13.el5 - xinetd-2.3.14-16.el5

- Group: System Environment/Daemons
- Summary: A secure replacement for inetd.
- Description: Xinetd is a secure replacement for inetd, the Internet services daemon. Xinetd provides access control for all services based on the address of the remote host and/or on time of access and can prevent denial-of-access attacks. Xinetd provides extensive logging, has no limit on the number of server arguments, and lets you bind specific services to specific IP addresses on your host machine. Each service has its own specific configuration file for Xinetd; the files are located in the /etc/xinetd.d directory.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

xkeyboard-config-0.8-9.el5 - xkeyboard-config-0.8-10.el5

- Group: User Interface/X
- Summary: xkeyboard-config alternative xkb data files
- Description: xkeyboard-config alternative xkb data files
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xmlrpc-c-1.16.24-1206.1840.el5 - xmlrpc-c-1.16.24-1206.1840.4.el5

- Group: System Environment/Libraries
- Summary: A lightweight RPC library based on XML and HTTP
- Description: XML-RPC is a quick-and-easy way to make procedure calls over the Internet. It converts the procedure call into XML document, sends it to a remote server using HTTP, and gets back the response as XML. This library provides a modular implementation of XML-RPC for C.
- Added Dependencies:
  - curl-devel >= 7.15.5-15
- Removed Dependencies:
  - curl-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-drv-i810-1.6.5-9.36.el5 - xorg-x11-drv-i810-1.6.5-9.40.el5

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 i810 video driver(s)
- Description: X.Org X11 i810 video driver.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-drv-mga-1.4.13-2.el5 - xorg-x11-drv-mga-1.4.13-5.el5

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 mga video driver
- Description: X.Org X11 mga video driver.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-drv-sis-0.9.1-7.3.el5 - xorg-x11-drv-sis-0.9.1-7.3.el5_7.1

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 sis video driver
- Description: X.Org X11 sis video driver.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-server-1.1.1-48.76.el5_6.4 - xorg-x11-server-1.1.1-48.90.el5

- Group: User Interface/X
- Summary: X.Org X11 X server
- Description: X.Org X11 X server
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

xulrunner-1.9.2.18-2.el5_6 - xulrunner-1.9.2.26-1.el5_7

- Group: Applications/Internet
- Summary: XUL Runtime for Gecko Applications
- Description: XULRunner provides the XUL Runtime environment for Gecko applications.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yp-tools-2.9-1.el5 - yp-tools-2.9-2.el5

- Group: System Environment/Base
- Summary: NIS (or YP) client programs.
- Description: The Network Information Service (NIS) is a system which provides network information (login names, passwords, home directories, group information) to all of the machines on a network. NIS can enable users to login on any machine on the network, as long as the machine has the NIS client programs running and the user's password is recorded in the NIS passwd database. NIS was formerly known as Sun Yellow Pages (YP). This package's NIS implementation is based on FreeBSD's YP and is a special port for glibc 2.x and libc versions 5.4.21 and later. This package only provides the NIS client programs. In order to use the clients, you'll need to already have an NIS server running on your network. An NIS server is provided in the ypserv package. Install the yp-tools package if you need NIS client programs for machines on your network. You will also need to install the ypbind package on every machine running NIS client programs. If you need an NIS server, you'll need to install the ypserv package on one machine on the network.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ypserv-2.19-5.el5_6.1 - ypserv-2.19-9.el5

- Group: System Environment/Daemons
- Summary: The NIS (Network Information Service) server.
- Description: The Network Information Service (NIS) is a system that provides network information (login names, passwords, home directories, group information) to all of the machines on a network. NIS can allow users to log in on any machine on the network, as

long as the machine has the NIS client programs running and the user's password is recorded in the NIS passwd database. NIS was formerly known as Sun Yellow Pages (YP). This package provides the NIS server, which will need to be running on your network. NIS clients do not need to be running the server. Install ypserv if you need an NIS server for your network. You also need to install the yp-tools and ypbind packages on any NIS client machines.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yum-3.2.22-37.el5 - yum-3.2.22-39.el5

- Group: System Environment/Base
- Summary: RPM installer/updater
- Description: Yum is a utility that can check for and automatically download and install updated RPM packages. Dependencies are obtained and downloaded automatically prompting the user as necessary.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yum-rhn-plugin-0.5.4-22.el5 - yum-rhn-plugin-0.5.4-26.el5

- Group: System Environment/Base
- Summary: RHN support for yum
- Description: This yum plugin provides support for yum to access a Red Hat Network server for software updates.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yum-utils-1.1.16-16.el5 - yum-utils-1.1.16-21.el5

- Group: Development/Tools
- Summary: Utilities based around the yum package manager
- Description: yum-utils is a collection of utilities and examples for the yum package manager. It includes utilities by different authors that make yum easier and more powerful to use. These tools include: debuginfo-install, package-cleanup, repoclosure, repodiff, repo-graph, repomanage, repoquery, repo-rss, reposync, repotrack, verifytree, yum-builddep, yum-complete-transaction, yumdownloader, yum-debug-dump and yum-groups-manager.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

zsh-4.2.6-5.el5 - zsh-4.2.6-6.el5

- Group: System Environment/Shells
- Summary: A powerful interactive shell
- Description: The zsh shell is a command interpreter usable as an interactive login shell and as a shell script command processor. Zsh resembles the ksh shell (the Korn shell), but includes many enhancements. Zsh supports command line editing, built-in spelling correction, programmable command completion, shell functions (with autoloading), a history mechanism, and more.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

Revision History

Revision 1-1.6.400	**2013-10-31**	**Rüdiger Landmann**
Rebuild with publican 4.0.0		
Revision 1-1.6	**Wed Nov 14 2012**	**Eliška Slobodová**
Included text of an asynchronous kernel erratum.		
Revision 1-0	**Thu Feb 21 2012**	**Martin Prpič**
Release of the Red Hat Enterprise Linux Technical Notes.		